NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

INCREASING THE CAPACITY OF A KNOWLEDGE INTENSIVE PROCESS THROUGH THE USE OF PROCESS REENGINEERING AND KNOWLEDGE-VALUE ADDED METHODOLOGIES

by

Errol A. Campbell, Jr.
Joseph L. Baxter, Jr.

June 2003

Thesis Advisor:	Thomas Housel
Associate Advisor:	Brian Steckler

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY	**2. REPORT DATE** June 2003	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: Increasing the Process Capacity of a Knowledge Intensive Process Through the use of Process Reengineering and Knowledge-Value Added Methodologies..	**5. FUNDING NUMBERS**
6. AUTHORS Errol A. Campbell, Jr. Joseph L. Baxter	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.	**12b. DISTRIBUTION CODE**

13. **ABSTRACT:** In the increasingly dynamic environment of information technology, it has become imperative that organizations continue to seek ways to effectively capture and measure knowledge in order to survive. With the emergence of a global economy and information networks, the knowledge creating capacity within organizations has grown tremendously. As a result, organizations are now shifting their focus to management of the knowledge used in executing processes and producing products. As demand for quality products and services continues to grow, companies must now find ways to effectively manage knowledge intensive processes in order to increase overall process capacity. Through business process reengineering and the KVA methodology, this thesis will seek to identify ways in which the performance of knowledge assets can be measured and make recommendations to improve the capacity of knowledge intensive processes, better enabling organizations to meet increased demand.

14. **SUBJECT TERMS** Information Assurance; Knowledge Value Added, KVA, Business Process Reengineering, BPR, Network Assessment, Knowledge Management, Knowledge Intensive Processes, Measuring Knowledge, Computer Network Vulnerability Team	**15. NUMBER OF PAGES** 115
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

THIS PAGE INTENTIONALLY LEFT BLANK

INCREASING THE PROCESS CAPACITY OF A KNOWLEDGE INTENSIVE PROCESS THROUGH THE USE OF PROCESS REENGINEERING AND KNOWLEDGE-VALUE ADDED METHOGOLOGIES

Errol A. Campbell, Jr.
Lieutenant, United States Navy
B.S., United States Naval Academy, 1995

Joseph L. Baxter, Jr.
Major, United States Marine Corps
B.S., Morehouse College, 1989

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 2003

Author:	Errol A. Campbell, Jr. Joseph L. Baxter
Approved by:	Thomas Housel Thesis Advisor
	Brian Steckler Associate Advisor
	Dan Boger Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In the increasingly dynamic environment of information technology, it has become imperative that organizations continue to seek ways to effectively capture and measure knowledge in order to survive. With the emergence of a global economy and information networks, the knowledge creating capacity within organizations has grown tremendously. As a result, organizations are now shifting their focus to management of the knowledge used in executing processes and producing products. As demand for quality products and services continues to grow, companies must now find ways to effectively manage knowledge intensive processes in order to increase overall process capacity. Through Business Process Reengineering and the Knowledge Value Added (KVA) methodology, this thesis will seek to identify ways in which the performance of knowledge assets can be measured and make recommendations to improve the capacity of knowledge intensive processes, better enabling organizations to meet increased demand.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS

CSS	Central Security Service
NSA	National Security Agency
NCPAC	NSA/CSS Pacific
CNVT	Computer Network Vulnerability Assessment Team
POC	Proof of Concept
IA	Information Assurance
IT	Information Technology
BPR	Business Process Reengineering
DoD	Department of Defense
KVA	Knowledge Value Added
KM	Knowledge Management
IW	Information Warfare
NCW	Network Centric Warfare
PACOM	Pacific Command
AOR	Area of Responsibility
TQM	Total Quality Management
ERP	Enterprise Resource Planning
SME	Subject Matter Expert
WT	Work Time
RLT	Relative Learn Time
ALT	Actual Learn Time
COCOM	Combatant Commander
SIPRNET	Secure Internet Protocol Routing Network
ROK	Return on Knowledge
ROIT	Return on IT

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGEMENTS

The authors would like to express their sincere gratitude to Dr. Thomas Housel and Professor Brian Steckler for their assistance, guidance and professional wisdom throughout the process of developing this thesis.

I would like to extend my personal thanks to the professionals of the NCPAC CNVT for their patience and cooperation during the past year. To the Baxter family, thank you for the support you have given to Joe and I, and for your understanding when Joe couldn't be there with you. To the Lemott's, thank you for keeping me well nourished over the past quarter and helping me stay focused when I wasn't seeing too clearly. Lastly, to my beautiful wife Tamara, thank you for sharing your experience and insight with me. My experience during this thesis and here at NPS would not have been the same without you here!

Errol

My heartfelt thanks to the many professionals that contributed to this endeavor. The guidance received from our advisors and professors will undoubtedly contribute to any future successes attained. My thanks also to the CNVT personnel for taking the time to make sure we understood their processes and for being straightforward with us. Personally, I wish to thank my family for their patience and support. Finally, my thanks to my partner for keeping us above water when the seas got rough!

Joseph

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PURPOSE

The purpose of this research is to examine a methodology to increase the process capacity of knowledge intensive organizations through objective measurement and valuation of deployed knowledge. The National Security Agency / Central Security Service (NCPAC) Computer Network Vulnerability Team (CNVT) network assessment process is examined as a Proof of Concept (POC). This process is conducted within the complex, knowledge intensive environment of Information Assurance (IA). Application of this model to a knowledge intensive organization provides insight into the relationship between the value created through knowledge and the processes in which knowledge is deployed, thus contributing to the effective management of knowledge assets and an overall increase in process capacity. Through research and critical analysis, this thesis will seek to capture the value-adding performance of knowledge assets deployed within the CNVT core processes and attempt to identify ways in which process capacity can be increased.

B. BACKGROUND

As the 21st century begins to take shape, we are witnessing the transition to a "new" economy[1], characterized by information technologies, global markets and new communications networks such as the internet. In this fast developing, ever changing environment, value creation within organizational processes has taken on new meaning. Increased access to information has developed intellectual assets within an organization that contribute significantly to overall value, prompting a shift towards more knowledge-based organizations where management of knowledge is fast becoming the norm. As a result, traditional methods of valuation that measured fixed, tangible assets, such as plant equipment, machinery and dollars, no longer present a complete measure of value and Knowledge Management has become a primary method of creating value from an otherwise intangible asset (Krishna, 2000; Housel and Bell, 2001). In order for these

[1] The new economy is often referred to as the Information Economy. Information now has the superior role, rather than material resources or capital, in creating wealth. (Kelly, 1997)

knowledge-intensive organizations to continue to thrive, the growing consensus is that they must continue to excel at value creation and knowledge management. This has led to an increased interest in intellectual capital, competency assessments, and the development of organizational assessments and has spawned the need to objectively measure the value of knowledge within an organization (Conger, et al. 1999).

While searching for means of more effective measurement of knowledge, firms must also recognize how to deploy it efficiently. With the customer at the center of an enterprise's business strategy, business processes must be fast, focused and flexible to ensure survival in the new economy (El Sawy 2001). It is not enough for companies to just share data, information, and knowledge; this sharing must be centered on core processes to ensure maximum value creation. Furthermore, as customer demand for quality products and services continues to grow, companies need to find ways to effectively manage knowledge intensive processes in order to increase overall process capacity to meet the demand. This requires growing intellectual capital and property and then discovering how to deploy those assets in the most effective manner (Conger, et al. 1999). Through application of our chosen methodology, this thesis will seek to demonstrate how the performance of knowledge assets can be measured and make recommendations to improve the capacity of knowledge intensive processes.

C. AREA OF RESEARCH

Based on the literature review, our supporting research can be divided into four main areas:

1. Knowledge Management

As Information Technology (IT) continues to foster the growth of knowledge, knowledge management has become a key element of an organization's strategy. In this section, we will identify reasons why many measures of knowledge management fail to provide companies the information that is needed to help increase process capacity, and discuss the role that IT should play in formulating a more effective strategy.

2. Business Process Reengineering

Business Process Reengineering[2] (BPR) provides the detailed method to describe the processes where the CNVT knowledge assets are utilized. Research into BPR literature serves to help provide a general understanding of how the concept has evolved and examines existing frameworks and principles that can be useful in guiding efforts to increase the capacity of knowledge intensive processes.

3. NCPAC Computer Network Vulnerability Team

The purpose of this section is to provide background information on our proof of concept and identify the need for increased process capacity in this knowledge intensive organization. Network assessment methodology and stakeholders are introduced to support our research into applying BPR and knowledge management principles. A short discussion on Information Assurance is included to show the context within which the CNVT must function. Although not discussed in detail, to further support our research, applicable directives will be reviewed to define the procedures that Department of Defense (DoD) agencies must adhere to in implementing information assurance in their networks.

4. Return on Knowledge

We will also devote a section of the thesis to discussion of the Knowledge Value Added (KVA) methodology and why it was chosen as our method of knowledge valuation. KVA is a way to objectively capture and measure the relationship between knowledge and its associated value within a set of processes and provides the framework from which the value-adding performance of knowledge assets can be measured. As this will be our methodology of choice during data analysis, the purpose of this section is to introduce the concept as well as the underlying principles on which it is founded.

Lastly, the data collection and analysis sections of the thesis will be an application of BPR principles and the KVA methodology. As a proof of concept, we will apply the BPR and KVA knowledge management tools to the network assessment process of the CNVT. We will conduct a detailed audit of the major processes involved in conducting a

[2] "BPR is in essence a performance improvement philosophy that aims to achieve quantum improvements by primarily rethinking and redesigning the way that business processes are carried out." (El Sawy. P. 6)

CNVT network assessment and measure the performance of the knowledge assets utilized throughout. Core processes will be modeled to allow for comparison of Return on Knowledge (ROK) before and after proposed changes. This case will culminate in the recommendation of ways to increase the overall process capacity of the CNVT.

D. SCOPE OF THESIS

The scope of our thesis will encompass BPR for knowledge intensive processes in the Information Assurance context. The requirement for network security continues to grow as Information Warfare (IW) becomes a mainstream avenue of attack. The transformation to Network Centric Warfare[3] (NCW) has thrust the Department of Defense into the Information Age and emphasis on Information Assurance has become a critical element of success. The NCPAC CNVT is a key contributor to the success of DoD's IA initiatives. Operating within the Pacific Command (PACOM) Area of Responsibility (AOR), the team conducts network assessments that attempt to identify shortfalls or vulnerabilities of PACOM's numerous networks. These assessments result in recommendations designed to enhance network security and increase provisions for IA. Since the CNVT is a relatively small unit, its services are continuously in high demand. As such, it is vital that the team be utilized in such a way that maximizes their process capacity and overall efficiency. Using process reengineering and the Knowledge Value Added methodology, this thesis will provide recommendations for more efficient knowledge asset utilization to increase the overall process capacity of the CNVT.

The concepts applied in this thesis are not specific to CNVT processes. Our POC is used to serve as an example of how BPR and KVA can be applied to improve a knowledge intensive process. The concepts and ideas applied in this thesis can be used throughout DoD and other agencies in which knowledge intensive processes are prevalent.

[3] NCW is that concept that fulfils the goal as set forth in the Joint Vision 202 document that mandates that DoD pursue information superiority in that joint forces may possess superior knowledge and attain decision superiority across any spectrum of conflict (DoD Report to Congress on "Network Centric Warfare", 27 July, 2001.).

E. ORGANIZATION OF THESIS

The remainder of this thesis is organized into five chapters. Chapter II will consist of a literature review to include overviews of the Knowledge Management / Business Process Reengineering arenas and their impact on a knowledge intensive organization and the CNVT need for increased process capacity. Chapter III will consist of a discussion of the KVA methodology, as it is our proposed knowledge valuation method. The next two chapters are devoted to our Proof of Concept. Chapter IV will be a discussion on collection of data and the methodology surrounding that collection. We will conduct a knowledge audit of “as-is” core processes to identify areas in which more effective knowledge deployment is likely to result in increased process capacity. In Chapter V we will model the proposed “to-be” processes and conduct ROK comparisons to the “as-is” processes. Our thesis will conclude with Chapter VI. Here we will include a general discussion of how we answered our research questions as well as provide CNVT specific and general recommendations that can be applied to knowledge intensive organizations throughout DoD.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

A. KNOWLEDGE MANAGEMENT

The importance of knowledge has been emphasized since Sun Tzu reflected on the role of information in warfare 2,500 years ago. In *The Art of War*, he writes:

> Know the enemy and know yourself; in a hundred battles you will never know peril. When you are ignorant of the enemy but know yourself, your chances of winning and loosing are equal. If ignorant of both your enemy and yourself, you are certain in every battle to be in peril.

While Sun Tzu's writings highlight the impact knowledge can have during war, this is not a concept unique to military organizations. Over the past decade, the notion of managing organizational knowledge has begun to dominate the business strategies of corporate America as well. The transition from the Industrial Age to the Information Age has brought about an evolution in management that shifts focus from managing people to managing the intellectual capital that this new knowledge era has brought about (Krishna, 2000). As Britton Manasco[4] writes in a *Knowledge, Inc*[5] article "The emergence of the knowledge era has left many corporate leaders feeling that something is disturbingly out of balance". Companies are now beginning to realize that their continued success depends on their ability to effectively leverage and manage their intellectual capital. Rather than reducing head count as a primary means of cutting cost, organizations are now finding ways to effectively and efficiently capture and share knowledge and expertise as a means of creating value. According to a recent benchmarking study by the American Productivity & Quality Center (APQC)[6], strategic efforts to manage and transfer knowledge more effectively have resulted in overall savings in excess of $700 million among major corporations that have implemented Knowledge Management solutions (Manasco, 1996).

[4] Britton Manasco is a market strategist with more than a decade of expertise developing compelling initiatives to assess markets and analyze business opportunities. His clients have included Microsoft/Great Plains, SAP, SAS, E.piphany, Trilogy, Peoplesoft, IBM, NCR, Motive and Vignette.

[5] *Knowledge Inc.* is a Web-based resource for executives who are developing their strategic change, technology and knowledge management initiatives.

[6] The American Productivity and Quality Center is based in Houston, TX. APCQ is an internationally recognized resource for process and performance improvement that helps organizations adapt to rapidly changing environments, build new and better ways to work, and succeed in a competitive marketplace.

While it is easy to recognize the benefits of pursuing knowledge management initiatives, such drastic reductions in bottom line numbers can only be achieved when it is implemented properly. With a firm's success dependent upon its ability to effectively manage and leverage knowledge assets, competitive focus has shifted from trying to "out-do" one another to trying to "out-know" one another (Housel and Bell, 2001, p1). While companies continue to make every effort to know more than the competition, they must ensure that knowledge management be implemented properly or the results can be disastrous. Stewart (2002) estimates that poorly managed knowledge costs Fortune 500 companies about $12 billion a year. Daniel Morehead, director of organizational research at British Telecommunications PLC in Reston, Va., suggests the failure rate of KM projects is close to 70 percent (Ambrosio, 2000). The high failure rate isn't a result of total failure. Rather it is the result of KM projects failing to achieve their stated goals – they don't accomplish what they set out to do because the right information is not delivered to the right people when it is needed. What managers are finding today is that, as knowledge management initiatives are thrust upon them more and more, the challenge still remains to successfully differentiate between intellectual capital that needs to be managed and leveraged and that which is of no value to an organization at all.

1. Knowledge Defined

Managing knowledge implies that one has defined what knowledge is and knows how to manage it. In the case of a financial advisor, for example, who in effect manages a client's financial assets, knowing how to allocate resources depends directly upon how the client's financial goals and objectives are defined and the advisor's knowledge[7] of the financial industry. For the Information Assurance professional, knowing how to assess and secure a network depends on how network security deficiencies are defined and his/her knowledge[8] of the industry. Similar examples can be cited for other management fields as well. However, to assist in understanding why knowledge management has risen

[7] In this example, knowledge of the industry implies an individual has had some type of formal education on the principles and practices of that particular industry and is considered somewhat well versed in the tricks of that trade.

[8] Ibid.

to the forefront of recent organizational initiatives, we must first develop an understanding of what knowledge is.

Throughout our literature review we found varying definitions of knowledge that all presented a common theme: knowledge is more than a simple extension of data and information. Data simply represents facts or observations out of context (Zack, 1999). Within organizations, data is more easily described as structured records of transactions that are usually stored in some sort of technology system (Davenport and Prusak, 1998). An example would be a sales database in which data is stored that represents various customer transactions with an organization. The data simply describes the facts of the transaction: when it was made; what the cost to the customer was; and how many items were purchased. They reveal nothing about why the customer chose to do business with that particular organization or whether they will chose to do business with them again. In effect, data by itself serves little purpose and provides minimal use.

Davenport and Prusak (1998) describe information as data that makes a difference. Zack (1999) defines information as that which results from placing data within some meaningful context. Both agree that information generally exists in the form of a message with the intent of conveying something useful from the sender to the receiver. Information is a form of communication that exists to make a difference in someone's outlook or provide further insight to the person receiving it. Unlike data, however, information has relevance and purpose. In fact, data becomes information when its creator adds meaning (Davenport and Prusak, 1998). When data is repeatedly transformed into information with some meaningful context, we begin to acquire knowledge – that which we come to believe based on the accumulation of information through experience and inference (Zack, 1999). Perhaps the most comprehensive definition of knowledge is that offered by Davenport and Prusak, which states:

> Knowledge is a fluid mix of framed experience, values, contextual information, and expert insight that provides a framework for evaluating and incorporating new experiences and information. It originates and is applied in the minds of knowers. In organizations, it often becomes embedded not only in documents or repositories but also in organizational routines, processes, practices, and norms.

This definition effectively captures the meaning of knowledge as it is used within the Information Assurance context. The intellectual capital of IA professionals is accumulated over years of experience, either from textbooks and training, or practical field application. As their expertise grows, so too does the framework from which they operate. As a result, information is used more effectively, and vulnerabilities and their respective remedies are easier to identify. Furthermore, the more this expertise is used, the more it becomes embedded within the different IA processes. Acquiring a complete and accurate definition of knowledge, however, doesn't assist in fully understanding why there is much difficulty in capturing and measuring the value of knowledge.

2. Facets of Knowledge

Throughout our literature review, several key facets of knowledge were identified. Knowledge can be classified either as explicit or tacit. Explicit knowledge is that which has been easily articulated and is simple to transfer from person to person. It is easier to codify and can normally be found shared in documents, databases and other tangible media. Unlike explicit knowledge, tacit knowledge is much more difficult to capture and share because it is subconsciously understood and developed from direct experience and action (Zack, 1999). Tacit knowledge is "deeply rooted in an individual's action and experience, as well as in ideals, values or emotions" that have developed within an individual (Nonaka and Takeuchi, 1995).

Housel and Bell (2001) offer even further insight into our understanding of knowledge. Born knowledge is that which is created within an organization to help it successfully engage a dynamic environment. This newly acquired knowledge may be either human or machine based and is generally focused on the survival and maximization of the organization. An example would be Intel's development of the Centrino processor for mobile computing or the development of the alloy for a lighter auto body.

Just as knowledge can be born within an organization, it can also die there. As an organization's environment changes and efforts are made to maintain competitive advantage, cost is generally the first area of focus. In most firms, cost is directly proportional to head count, and therefore downsizing becomes the primary means of reducing expenses. Based on pure logic, however, when downsizing with cutting costs in mind, firms typically look to their highest paid workers as prime targets, often neglecting the fact that those higher salaries are tied to the amount of knowledge resident in that worker. As a result, firms often find themselves with significantly less intellectual capital after periods of layoffs and have done more damage than good to the organization as a whole. (Housel and Bell, 2001)

Knowledge can also be privately owned. In today's global economy where maintaining competitive advantage is essential to an organization's survival, protection of privately held knowledge is more important now than it has ever been. Private, or proprietary, knowledge is what allows a firm to increase its wealth and maintain a foothold in the market place. It is not readily available to the public because it serves that particular organization's interest and is tied directly to their ability to remain competitive. Today, however, there are very few concepts and ideas that remain unique to an organization and are not generally available. As technology has made it easier and easier to mass-produce goods of like design and quality, companies are making increased efforts to ensure that proprietary knowledge remains private. Companies such as Coca-Cola, whose formula remains a trade secret even today, are rare (Davenport and Prusak, 1998). More often than not, we are seeing advantageous knowledge become readily available, such as what happened to Netscape's ownership of internet browsing technologies in the 1990's (Housel and Bell, 2001).

The success of a knowledge intensive organization hinges on its ability to manage knowledge. Identifying and capturing tacit knowledge is often the most difficult task because in knowledge intensive environments it involves knowledge that is expressed as action-based skills that are difficult to reduce to rules and recipes. As personnel come and go, the need to maintain a stable knowledge base is equally important. For a knowledge intensive firm, reducing head count as a primary means of cost cutting will not necessarily produce the desired results if the primary knowledge base is cut as well. Like all organizations, those that are knowledge intensive must also develop new ways of implementing KM projects while ensuring their own longevity.

3. Knowledge Valuation

An essential element of effective knowledge management is understanding how to measure its value. Knowledge intensive organizations are getting smarter as workers become empowered and encouraged to continuously learn. As more and more resources are committed to learning, management must find ways to capture the value of knowledge that is otherwise an intangible asset (Krishna, 2000). However, this challenge is quite difficult since traditional methods of economic valuation are based on fixed, tangible assets that are measured as capital investments. The knowledge embedded within core processes, employee brains, patents and copyrights are key contributors to an organization's competitive advantage. The effective measurement of these intangible assets has proven to be rather illusive. Today, with such intangible assets as the primary driver of corporate performance, assessing the investment in those resources has become even more crucial (Osterland, 2001).

Throughout our literature review there was mention of several different approaches to the dilemma of knowledge valuation. Perhaps the best summary is offered by Housel and Bell (2001) in which the most prevalent approaches and assumptions are discussed. Their summary is depicted in Table 1.

Method	General Assumption	What is Lacking
Process of elimination	Tangible and intangible assets can be separated. What is left is knowledge value	Does not focus on common unit of measurement for analysis of knowledge across entire organization.
It's in here somewhere	All encompassing approach that assumes the more indicators of intellectual capital you identify, the more complete your picture knowledge value is.	Does not identify which indicators should be most important to the manager
Everything is cost	Assumes the value of knowledge can be measured by calculating its market price	Market price does not directly translate to the value the knowledge creates
Rorschach (Ink Blot)	Assumes managers can derive the value of knowledge through intuitively related performance measures.	Interpretation is left to managers. Does not present consistent mathematical relationship among measures.
Forget it	Assumes it is impossible to develop meaningful measures since knowledge is intangible. Believes only the outputs of knowledge can be measured.	Does not establish a specific relationship between knowledge used and presumed outputs.
Knowledge is proportionate to value	Assumes a direct relationship between knowledge and the value it creates.	Does not identify the value embedded within creative knowledge assets

Table 1. Methods of Knowledge Valuation

With the general assumption that the deployment of a knowledge intensive organization's knowledge assets centers on core processes, the "knowledge is proportional to value" approach seems most appropriate. In the framework of this approach, the explicit knowledge deployed within the organization's processes is directly observable and common units of knowledge can be devised as surrogates to describe common units of process outputs (Housel and Bell, 2001). In our case, for example, the explicit knowledge deployed throughout the assessment process can be observed and captured in specific, common units of measurement. Since knowledge is proportional to value, it logically follows that the amount of knowledge deployed throughout the CNVT processes can be measured in common units and these units are surrogates for the process outputs or the value of the process (Housel and Kanevsky, 1995). The upshot is that, through this approach, we should be able to objectively measure value through the amount of knowledge deployed in network assessment processes.

4. The Role of IT

As the new millennium begins to unfold, knowledge continues to play an increasingly important role in an organization's strategy. The ramifications of confusing data, information and knowledge are becoming increasingly costly. Organizations have spent tremendous amounts of money on technology initiatives that have not delivered what was needed or promised (Davenport and Prusak, 1998). In today's economy where nothing is guaranteed and all is virtually uncertain, the only "sure source of lasting competitive advantage is knowledge"(Nonaka and Takeuchi, 1995). Organizations are becoming more knowledge intensive in which continuous learning is encouraged and, in fact, a necessary must for an employee to be successful. Take for example the Healthcare field. For years, healthcare professionals have trained to be able to recall and apply information pertaining to a specific illness. Now, with the influx of technology and global networking, they are required to manage more than just the knowledge within their own brains. They must also manage the internally generated knowledge about patients such as medical history and insurance information, as well as the knowledge made available through sharing across networks (Moore, 2002).

The amount of information generated now by IT in the Healthcare community and the resulting knowledge it creates qualifies it as knowledge intensive. A similar conclusion can be drawn for Information Assurance professionals since the crux of their existence is knowledge of the fundamentals of IT, its many vulnerabilities, and the solutions to correct them. As knowledge intensive organizations grow, so too does the complexity of the knowledge they are required to manage. Such organizations must be able to integrate and share highly distributed knowledge to ensure effective performance and continued growth (Zack, 1999). With the advent of the intranet and various networking technologies, cross-organizational knowledge sharing is not uncommon.

Companies can now access cross-platform information from various locations worldwide via the internet (Krishna, 2000). With such technology facilitating the sharing of information, the problem of deciding how to effectively deploy IT in a knowledge management solution warrants attention as well.

In understanding the role of IT in knowledge management, it should be emphasized that IT is an enabler rather than a driver (Krishna, 2000). Housel and Bell (2001) further highlight this by offering two fundamentals that, if followed, make moving knowledge assets to IT an advantageous endeavor. First, simple and procedural knowledge that is employed frequently should be moved to IT. Such tedious work as accounting, billing and basic manufacturing follows very specific rules. Moving this procedural knowledge to IT dramatically lowers the cost per usage of this knowledge. The second principle addresses one of the knowledge facets previously mentioned. Organizations should seek to capture in IT the knowledge that typically dies when an employee leaves the company. The critical complex knowledge that a worker has accumulated over years of experience is often essential to the continual smooth operation of the organization. Capturing it in IT ensures that the knowledge remains embedded throughout processes and is accessible to less experienced employees.

B. BUSINESS PROCESS REENGINEERING

The concept of Business Process Reengineering is no longer new to organizations. Since the 1980's tremendous investments in IT have yielded only marginal increases in productivity and performance. Some attribute this to the confusion between knowledge and information (Malhotra, 2000). Others claimed that measurements were too narrowly defined and could not be appropriately applied to a service economy. Another set of explanations claimed that IT itself was not implemented properly; that the user interfaces and software were not user friendly and that managers did not fully understand IT (El Sawy, 2001). After several more years of failed IT investments, corporate America began to shift its focus. No longer were they addressing non user-friendly IT issues. The focus shifted to organizational processes, structures and designs that were not work-friendly. They began to realize that their traditional organizational designs were contributing more to poor performance and productivity than poorly implemented IT systems. With that realization, companies began to seek new ways of doing business with hopes of yielding tremendous increases in performance. The desire for more effective cost cutting, faster cycle times and better customer responsiveness, and the methods of getting there, became known as business process reengineering (El Sawy, 2001).

There have been numerous publications on business process reengineering since the concept gained momentum in the early 1990's. Two of the better-known works appeared simultaneously, focusing on the importance of business processes and how IT could be used as an innovation and transformation tool. The first was an article by Thomas Davenport and James Short. In what they refer to as "The new industrial engineering", they define a recursive relationship between information technology and business processes. This relationship, depicted in Figure 1, essentially sates that one should think of information technology in terms of how it supports new or redesigned processes, rather than business functions. Recursively, business processes and improvements should be thought of in terms of the capabilities that information technology could provide.

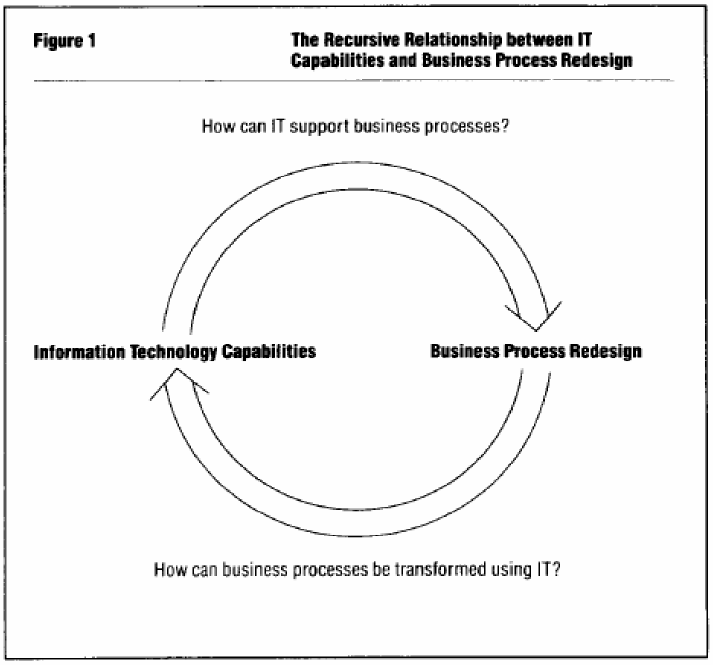


Figure 1
The Recursive Relationship between IT Capabilities and Business Process Redesign
How can IT support business processes?
Information Technology Capabilities
Business Process Redesign
How can business processes be transformed using IT?

Figure 1. Recursive Relationship Between IT and BPR (From: Davenport and Short, 1990)

The second work, an article by Michael Hammer, took a more radical approach to make the same argument. Rather than simply "webifying" or automating your old processes with IT, his message was to get rid of the old rules, begin anew with a clean slate and use IT to radically change the way your business is done. In essence, his approach sought to challenge the pre-existing assumptions inherent in the work process by forcing the notion of "discontinuous thinking" (Malhotra, 1998). Both approaches seek to redefine the way business is done through the use of IT and both have served as the foundation for the numerous BPR initiatives existing throughout corporate America today. Within the military and other organizations throughout DoD where operational capability must be maintained, Hammer's approach is not always a feasible option in guiding process redesign efforts. Many DoD entities are governed by external agencies such as the Defense Finance and Accounting Service (DFAS) and the Office of Management and Budget (OMB), or, in the case of Information Assurance, a myriad of policies and guidelines that must be followed, to ensure conformity with established laws. Therefore, radical change is particularly difficult on any scale. Additionally, established levels of readiness must be maintained throughout any type of reengineering processes. Maintenance of established levels of readiness and conformance with guidelines are measures used to evaluate DoD leadership. It is therefore difficult to convince commanders or leadership to conduct any type of reengineering effort that may be considered radical.

1. BPR Defined

Throughout our literature research, we were presented with several different definitions of business process reengineering. Despite the various flavors of BPR, the commonality is that the concept is more a process improvement philosophy whose primary focus is achieving improvements by rethinking and redesigning the execution of business processes (El Sawy, 2001).

Davenport & Short (1990) define business processes as "a set of logically related tasks performed to achieve a defined business outcome". Fundamentally, these processes have two important characteristics: they have customers and they span across organizational boundaries. Customers are the recipients of the business process outcomes and can be internal or external to an organization. Business processes are generally independent of organizational structure and can occur across and within the organizational subunits. Furthermore, processes can be large scale, affecting the whole organization or group, or more detailed such as completing a quarterly billing statement.

El Sawy (2001) defines a business process as "a coordinated and logically sequenced set of work activities and associated resources that produce something of value to the customer". Along with the common theme of being cross organizational and customer based, he adds that there are several other properties fundamental to business processes. They create knowledge and information flow around the process. Business processes can exist in multiple versions rather than one size fits all. Lastly, the degree of structure of a process can vary from highly structured for process with well-defined steps, to loosely structured for those that include knowledge intensive work. Regardless of which definition is chosen, a process redesign initiative driven by IT can be applied.

To fully illustrate how BPR fits into an organization, El Sawy uses the Leavitt Diamond.[9] In short, it is a depiction that shows that it simply is not enough to just redesign processes. It should be understood that, in order to maintain a sense of balance and stability within the organizations, the environment around the processes might need to be adjusted if the process redesign efforts are to be effective.

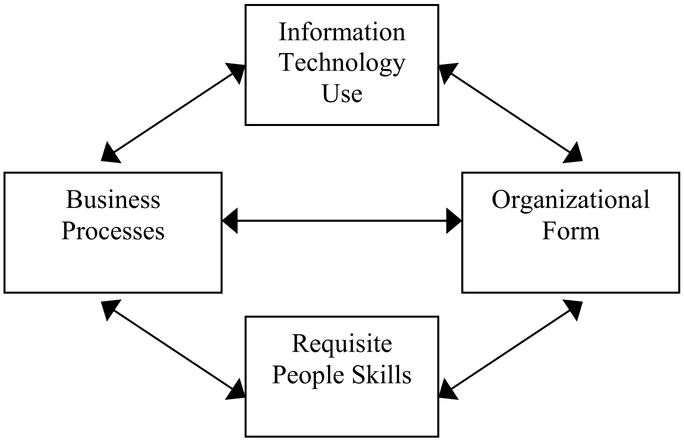


Figure 2. Leavitt Diamond

[9] Developed by H.J. Leavitt (1965), the diamond is used as an organizational model for illustrating the influences of technology, tasks, people and structure within an organization.

Figure 2 shows the Leavitt diamond, which presents a conceptual framework for balancing IT-enabled transformation. During a process redesign effort, when any of the four organizational variables is changed, the other three must be adjusted accordingly to ensure the organization maintains its functional harmony. As an example, if new information technology is introduced, business process will need to be adjusted to take advantage of it. As business processes change, newer people skills may be required to execute them, possibly resulting in a newer, more efficient organizational form (El Sawy, 2001). Understanding such a framework is critically important when redesigning processes that are knowledge intensive. As processes change, creating the need for new people skills or organizational form, the knowledge about those processes changes as well. It either departs with outgoing personnel or becomes useless because it resides in the mind of a person who is no longer associated with the process. Thus when redesigning processes, it is imperative to ensure that the knowledge about the process is considered.

2. BPR in Knowledge Management

Since the Total Quality Management (TQM) era reached its peak in popularity in the early 1980's the quest to improve an organization's performance has gone through several phases. After TQM came what El Sawy calls the first wave of BPR, built on the principles of Davenport and Short's "New Industrial Engineering" and Hammer's "Don't Automate, Obliterate" approach. As BPR transformation movements took place, the internet and the World Wide Web took off, eventually providing ubiquitous global connectivity and spawning the development of web-based business processes. Organizations began to redesign their processes to focus more on value chain management. As the next phase of BPR begins to unfold, the focus has shifted once again. With web technologies at the foundation of e-commerce, the knowledge creating capabilities of business processes is tremendous. As a result, organizational strategies and BPR efforts of today are centered on effectively managing the knowledge and value created by new processes. Table 2 summarizes the evolution of business process redesign efforts. As can be seen, the use of the internet as a core element of information technology infrastructure has facilitated the easy exchange of information and creation of knowledge around processes (El Sawy, 2001). As advances in technology continue to spawn new knowledge creating capabilities in organizations, the challenge of harnessing the value of knowledge will become increasingly difficult.

			Second-wave BPR		
	Total quality management	**First-wave BPR**	**Time-based Competition**	**Web-enabled e-business**	**Knowledge management**
Signature of process change	Reduction of variability and defects in process outputs	Obliteration of old task-oriented processes and replacement with radically innovated business processes	Transformation of process flows and organization to be fast, focused, and flexible	Cross-enterprise internet processes with suppliers, customers, and partners	Expanding the knowledge creation capacity of business processes
Nature and magnitude organizational change	Continuous incremental improvement	Espoused radical change - although often with incremental implementation	Cycle time used as a diagnostic for strategic organizational change	Collaborative business process redesign around cross-enterprise electronic interfaces	Knowledge change creates competencies for both improved and new processes
Associated Era	1980s	Early 1990s	1990s and beyond	Late 1990s and beyond	2000 and beyond
Role of IT	Minor role in data collection and analysis	Critical enabler of new ways of executing processes	Enabler of fast response	Web-based IT infrastructure enables new supply chain processes	Triggers the shaping and synthesis of new knowledge
Execution Approach	Bottom-up grass roots	Top down and mostly one-shot	Top down and comprehensive	Cross-Enterprise Partnering	Middle-Up-Down
Dysfunctional aspects or bad practices	Not necessarily strategic	Slash and burn downsizing	Not linking cycle time reduction to strategy	Few standardized partner interface processes	Confusing knowledge with information and data
Time frame of target focus	Continuing	Short-term performance focus	Long-term performance focus	Short-term and long-term performance focus	Long-term potential focus

Table 2. Evolution of BPR

3. BPR Principals

Several principals of process redesign have been introduced and dominated BPR efforts since the concept's inception. Hammer argued that process redesign efforts should break away from the outdated rules that governed operations because they were based on assumptions about technology, people and organizational goals that were no longer true (Malhotra, 1998). He proposed the following principals for process reengineering: (a) Organize around outcomes, not tasks; (b) have those who use the output of the process perform the process; (c) Subsume information-processing work into the real work that produces the information; (d) Treat geographically dispersed resources as though they were centralized; (e) Link parallel activities instead of integrating their results; (f) Put the decision point where the work is performed; (g) Capture information once and at the source. While Hammer's principles are appropriate for organizations that are prepared to embark on such an all-or-nothing journey, they offer no middle ground for firms that are bounded by external constraints or lack the time and resources to commit to such radical redesign.

In taking a much broader view, Davenport and Short (1990) propose principals that view IT as more than just an automating force. As illustrated in their recursive relationship (Figure 1), IT should provide capabilities to support business processes, and business processes should be in terms of what IT can provide. They propose a five-step method for redesigning business processes, shown in Figure 3.

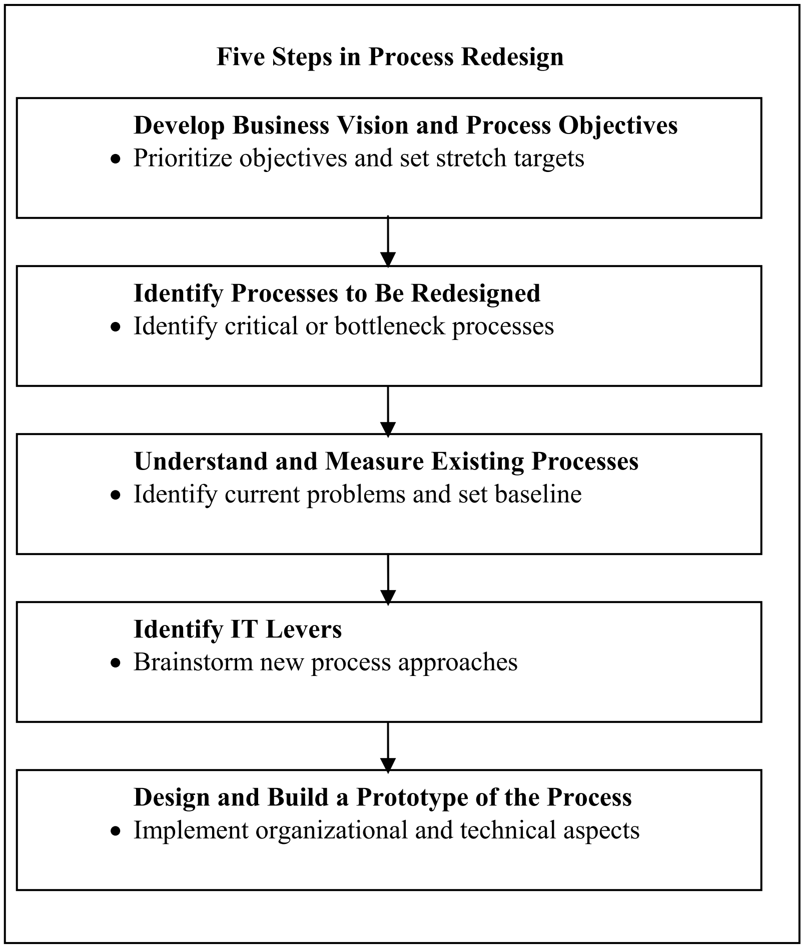

Five Steps in Process Redesign
Develop Business Vision and Process Objectives
• Prioritize objectives and set stretch targets
Identify Processes to Be Redesigned
• Identify critical or bottleneck processes
Understand and Measure Existing Processes
• Identify current problems and set baseline
Identify IT Levers
• Brainstorm new process approaches
Design and Build a Prototype of the Process
• Implement organizational and technical aspects

Figure 3. Five-Step Redesign Process (From: Davenport and Short, 1990)

An important point to highlight is that in identifying processes to be redesigned, the means by which processes are identified is critical. Since managers typically do not think of their business operations in terms of processes, this is often the most difficult step. Two major approaches are proposed: exhaustive and high impact. The exhaustive approach is generally the lengthiest, and often results in the most failures, because it attempts to identify *all* processes within an organization and prioritize them based on redesign urgency. Companies that have pursued this approach generally have not had the resources to address all of the identified processes. The high impact approach identifies only the most important processes or only those that are in the most conflict with the business strategy and objectives. This approach is generally more successful than the exhaustive approach because most companies have fairly good sense of which processes are most crucial to their success or are not in alignment with their overall vision.

With the continued broadening of the global economy and e-commerce quickly becoming a key pillar of enterprise business strategies, the redesign of processes for e-business has developed as a key area of concern. In the e-business environment, the capabilities afforded by e-commerce are giving competitive advantage to those corporations willing to exploit its full potential. Furthermore, enterprise partners, suppliers, and customers are demanding the same e-business capabilities. To meet such increasing demands and maintain competitive advantage, organizations are scrambling to transform their processes. El Sawy (2001) calls this "the e-business speed loop" (Figure 4) and uses it as a framework for developing a set of principles to guide enterprise process redesign efforts for e-business.

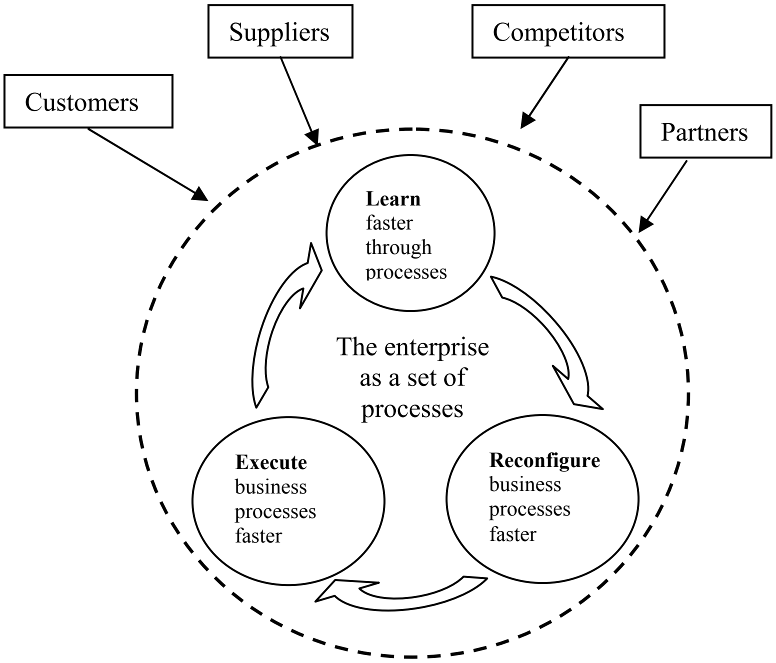

Suppliers
Competitors
Customers
Partners
Learn faster through processes
The enterprise as a set of processes
Execute business processes faster
Reconfigure business processes faster

Figure 4. e-Business Speed Loop (From: El Saway, 2001)

In the framework of the e-business speed loop, organizations have three sets of strategic capabilities that feed into each other, allowing them to compete and quickly exploit now opportunities offered by e-business. El Sawy offers ten redesign principles that enable quick execution of the strategic capabilities and encompasses all of the other redesign principles previously discussed:

(1) Streamline – Remove waste, simplify and consolidate similar activities.
(2) Lose Wait – Squeeze out waiting time in process links to create value.
(3) Orchestrate – Let the swiftest and most able enterprise execute.
(4) Mass-Customize – Flex the process for any time, any place, any way.
(5) Synchronize – Synchronize the physical and virtual parts of the process.
(6) Digitize and Propagate – Capture the information digitally and propagate it throughout the process.
(7) Vitrify – Provide glass-like visibility through fresher and richer information about process status.
(8) Sensitize – Fit the process with vigilant sensors and feedback loops that can prompt action.
(9) Analyze and synthesize – Augment the interactive analysis and synthesis capabilities around a process to generate value added.

(10) Connect, Collect, and Create – Grow intelligently reusable knowledge around the process through all who touch it.

It is our belief that combining Davenport and Short's five-step process with some of the key principles offered by El Sawy afford the best opportunity for a successful BPR initiative within the knowledge intensive context. An effective knowledge intensive organization is organized around tasks, rather than outcomes as proposed by Hammer. Furthermore, given the dynamic environment within which these organizations must operate, it is not always feasible to have those who benefit from the outputs of the processes actually perform the process. In Davenport and Short's five-step proposal, objectives and major bottleneck processes are easy to identify. As such, existing problems should be highly visible making it easier to brainstorm for new process approaches.

El Sawy's, e-business speed loop most accurately depicts the nature of the environment in which knowledge intensive organizations operate. Within their enterprise processes, the three strategic capabilities must be constantly balanced with meeting the needs of stakeholders – customers, suppliers, competitors and partners. To maintain that state of balance, any reengineering effort must incorporate most, if not all, of the principles proposed by El Sawy. Our POC case will demonstrate how this can be done while increasing process capacity as well.

4. Why BPR Fails

Despite the existence of clearly defined guidelines and numerous models from which to follow, 70 percent of all BPR projects fail (Malhotra, 1998). The reasons for such failures vary, but from among different experts on the topic there are several recurring themes. The most common are lack of sustained management commitment and leadership, and resistance to change. In most redesign efforts, the processes to be redesigned cut across various parts of the organization. If the redesign effort is being driven by a single subunit within the organization, it will more than likely encounter some resistance from other parts of the organization. Without strong, visible commitment from senior leadership[10], employees throughout the organization will not understand the

[10] "It is often said that major change is impossible unless the head of the organization is an active supporter" (Conger, et al. 1999. p. 90).

critical nature of the redesign effort or the role of IT within process redesign, and the customer's opinion as the recipient of the process output will be neglected.

Unrealistic scope and expectations also continue to doom process-reengineering efforts. Most organizations take on BPR initiatives with the hopes of seeing immediate and dramatic improvements in productivity and performance. Where they fail is ensuring that the appropriate processes are identified and the correct measures are taken to redesign them. Companies are expending tremendous financial resources on enterprise resource planning (ERP) systems from various BPR vendors with the expectation that the systems will provide regimented sharing of data across various business functions (Malhotra, 2000). These systems focused primarily on coordination of the company's internal functions. While they were successful at providing top-down data sharing within internal functions, the models were not scalable and did not allow for the multi-direction inter-organizational information flows with suppliers and customers needed to support e-business functions.

Some of the less prevalent but equally important causes of BRP failure are: too many projects under way; unsound financial position; not focusing on processes; spending too much time analyzing the current situation; ignoring concerns of your people; proceeding without strong executive leadership; over emphasis of the tactical aspects at the expense of strategic dimensions being compromised (Hammer and Stanton, 1995; Bashein et al., 1994; King, 1994).

There are, however, some tactics and preconditions that facilitate successful implementation of BPR initiatives. Bashein et al. (1994) outlines several preconditions for BPR successes: Senior management commitment; realistic expectations; empowered and collaborative workers; strategic context of growth and expansion; shared vision; sound management practices; full time participation of appropriate people. As the BPR initiative is implemented, there are several measures that leadership can take to help ensure it is done successfully. As with any organizational change, communication is critical. Management should communicate changes as clearly and succinctly as possible so that all involved have to same level of expectations. Anticipation of resistance, and appropriate measures to counter it, is an effective measure as well. Regular training sessions to discuss new procedures or policy facilitates communication and ensures that all concerns are addressed, helping to combat resistance. Lastly, management should ensure that goals to be achieved and the metrics by which they are measured are unambiguous and clearly defined[11].

C. COMPUTER NETWORK VULNERABILITY TEAM

The POC case examined in this thesis deals with finding a way to increase process capacity though objective measurement of value in the core processes of the NCPAC CNVT. The team's success is directly dependent on its ability to effectively coordinate, plan, and execute missions. Doing so requires repeated refreshment and application of team members' knowledge throughout the entire network assessment process. With increasing demand for the team's services and the dynamic nature of the information assurance field, the NCPAC CNVT qualifies as a knowledge intensive organization that could benefit from more efficient knowledge management facilitated by application of business process reengineering principles and information technology.

1. Overview

CNVT's purpose is to provide customers within the Pacific Command (PACOM) area of responsibility (AOR) the support necessary to "develop the best possible information system security posture through cooperative examination of their computer network systems. [This is done] through cooperative examination of their systems to identify and help counter vulnerabilities which could be exploited by an adversary" (CNVT Charter). The CNVT currently consists of 4 permanent NSA team members and is normally augmented with information assurance specialists from the USPACOM's Computer Network Defense and Information Assurance Division (J-65) and NSA's Network Security Evaluations and Tools Division (C-44). The team conducts ten to fifteen network vulnerability assessments per year and is seeking ways to increase their process capacity in order to allow them to meet increased demand for their services. Generally, the team will employ the following typical network assessment techniques to evaluate the networks and hosts within an AOR:

[11] In addition to preconditions for BPR discussed by Bashein, Conger, Spreitzer, and Lawler cite a list if eight steps to transforming an organization. (Conger, et al, 1999. p.99)

- Examine network configurations and documentation and become familiar with the architecture of customer infrastructures
- Examine and evaluate the Access Control configuration of perimeter routers and firewalls
- Examine and evaluate the Access Control configuration of Remote Access Systems
- Evaluate DMZ policies and configuration
- Examine services provided to internal and external customers (web, email, file sharing, etc.)
- Scan and evaluate key network servers and infrastructure devices
- Scan and evaluate all hosts for network and operating system vulnerabilities
- Verify latest patches and service packs are properly installed
- Examine password policies
- Evaluate physical security

2. IA

To be successful at the mission specified in their charter, team members must keep their knowledge current in the dynamic world of Information Assurance. Advances in technology require that members be aware of vulnerabilities and be familiar with associated remedies to ensure sustained security and IA. The ever-increasing automation, speed, and sophistication of network attack tools[12] warrants having Subject Matter Experts (SME) in network security. The threat to DoD network infrastructures is constant and requires regular refreshment of knowledge. Therefore, the knowledge resident within the team must be constantly updated. The CNVT is where the knowledge concerning IA resides, as they are the Pacific COCOM's group of network security SME.s.

Recognizing the immense challenges of maintaining IA, the DoD has issued a number of directives focused on ensuring data and Information Systems are secure. Entities such as the CNVT are created and relied upon to meet the requirements of laws and directives such as the Title 10, United States Code, Section 224, which establishes

[12] Department of Defense brief on "Safety and Security Extensions to iCMM and CMMI" 20 June 2002.

the requirement for a Defense Information Assurance Program, and the DoD Directive 8500 series, which establishes policy and assigns responsibilities to achieve IA within DoD infrastructures.

New operating systems[13], applications, connection media and increases in connection speeds, usage of satellite assets (both owned or leased), wireless peripherals, and automation advancements in general require constant education. The characteristics of IA, constant change and a multitude of sub processes that require expertise, make it a knowledge intensive process. As such, the CNVT, and entities like it, are all groups that can benefit from an applied methodology that helps increase process capacity within knowledge intensive organizations.

3. Stakeholders

There are several stakeholders in CNVT's network assessment process who continually influence its "e-business speed loop" (El Sawy, 2001). They range from the customers within the PACOM AOR, who are the most direct recipients of CNVT's process outputs, to the Combatant Commander who has the added assurance of knowing his networks are secure. Other stakeholders include but are not limited to:

- NSA's Network Security Evaluations and Tool Division – provides augmentation personnel for CNVT missions. Gain real world experience from mission planning and execution.
- USPACOM's Computer Network Defense and Information Assurance Division – provides augmentation personnel for CNVT missions. Gain real world experience from mission planning and execution.
- US Naval Postgraduate School Information Warfare Program - provides augmentation personnel for CNVT missions. Allow students to gain real world experience from mission planning and execution. Provide thesis opportunity for topics related to Information Assurance.

[13] The SANS Institute cites that the majority of successful attacks on operating systems come from only a few software vulnerabilities. Operating System vulnerabilities are the most exploited weaknesses by hackers because attackers are opportunistic, take the easiest and most convenient route, and exploit the best-known flaws with effective and widely available tools. These flaws are also the easiest to address and fix by applying updated patches. (SANS Institute Web site. www.SANS.org).

- USPACOM's Information Operations Division – provide funding assistance for CNVT missions in direct support of USPACOM operational objectives.

The Area of Responsibility covered by the CNVT extends from Japan to the entire West Coast of the United States and includes every point in between. It covers all geography within the Pacific, Arctic, and Indian Oceans and reaches North to include Alaska and South to include Australia.

D. RESEARCH QUESTIONS

The review of relevant literature suggests that management of knowledge within an organization is critical to survival in today's global economy. Like other for-profit organizations that rely on knowledge to maintain competitive advantage, DoD relies on organizational knowledge to maintain an advantage in the Information Assurance arena. However, unlike other organizations, this advantage is not tied directly to the ability to garner more market share or generate more sales revenue. Rather, it is tied to the ability to effectively provide service, support, and security of its information networks. Based on this understanding, and the needs identified throughout the literature review, the following primary and secondary research questions will be addressed:

1. Primary

a) Can the Capacity of Knowledge Intensive Processes Be Increased by Applying BPR and Knowledge Management Principles?

2. Secondary

a) Is There a Way to Objectively Measure the Value of Knowledge Deployed Within Knowledge-Intensive Processes?

b) Can Repeatable Processes Be Automated or Outsourced to Increase the Capacity of the CNVT?

THIS PAGE INTENTIONALLY LEFT BLANK

III. MEASURING THE RETURN ON KNOWLEDGE

This chapter describes a theory and methodology for estimating return on knowledge[14] that uses knowledge in people and technology as a way to describe process output in common units and also treats process outputs as value. The return on knowledge is captured by: (1) measuring the amount of knowledge used in a process to produce outputs, and (2) measuring the costs incurred in acquiring and applying this knowledge to produce these process outputs. The result is a common unit of knowledge that is a surrogate for common units of process output across the entire organization and a relationship of knowledge to value that helps resolve the question of how much value that knowledge provides to the organization. (Housel and Bell, 2001).

A. THEORY

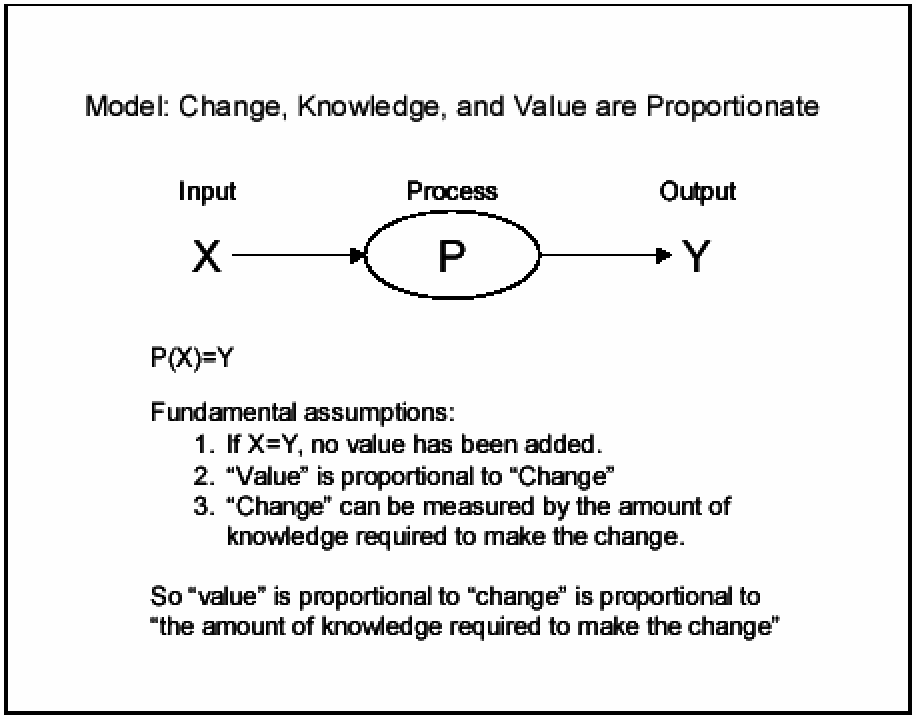
As previously mentioned, there have been numerous approaches to measuring the value of knowledge, each replete with their own strengths and weaknesses. Among them, the commonality is that none offer the manager a means of objectively measuring knowledge and its value across the entire organization. These methods of valuation rely on traditional financial indicators that do little to link knowledge to sub-corporate measures of performance (Strassman, 1999). Furthermore, these traditional methods neglect to incorporate information and the knowledge provided by IT into the performance metrics that are used by decision makers.

1. Knowledge Value Added

The Knowledge Value Added (KVA) methodology will be used in this thesis as a method of capturing the value of explicit knowledge within a knowledge intensive organization. The method, developed by Drs. Thomas J. Housel and Valery Kanevsky, provides a means for objective measurement of the relationship between knowledge and the value it produces in organizational processes and falls into the "knowledge is proportional to value" framework discussed in the literature review. By translating knowledge utilized into numerical form, KVA allows corporations to allocate revenue in

[14] For our purposes, Knowledge can be defined as a conceptual (ideational) construct generated through the agency of the human mind. (Housel and Bell, 2001) It is a surrogate for the process outputs measured in common units.

proportion to the amount of value added by knowledge (Housel and Bell, 2001). This methodology also proves beneficial to non-profit organizations because it presupposes knowledge as a surrogate for value and therefore can be used independent of profit generation. For this reason, and because cutting costs and reducing head count were not viable options for our proof of concept, KVA was chosen because it enables managers to measure the performance of corporate knowledge assets whether the knowledge is deployed in IT or resident within employees' heads. The methodology provides an aggregation of knowledge contributions within specific processes and indicates to decision makers areas in which efforts to increase productivity could be focused rather than simply focusing on cutting costs. The underlying assumptions of the KVA model are depicted in Figure 5.



Model: Change, Knowledge, and Value are Proportionate

P(X)=Y

Fundamental assumptions:

1. If X=Y, no value has been added.
2. "Value" is proportional to "Change"
3. "Change" can be measured by the amount of knowledge required to make the change.

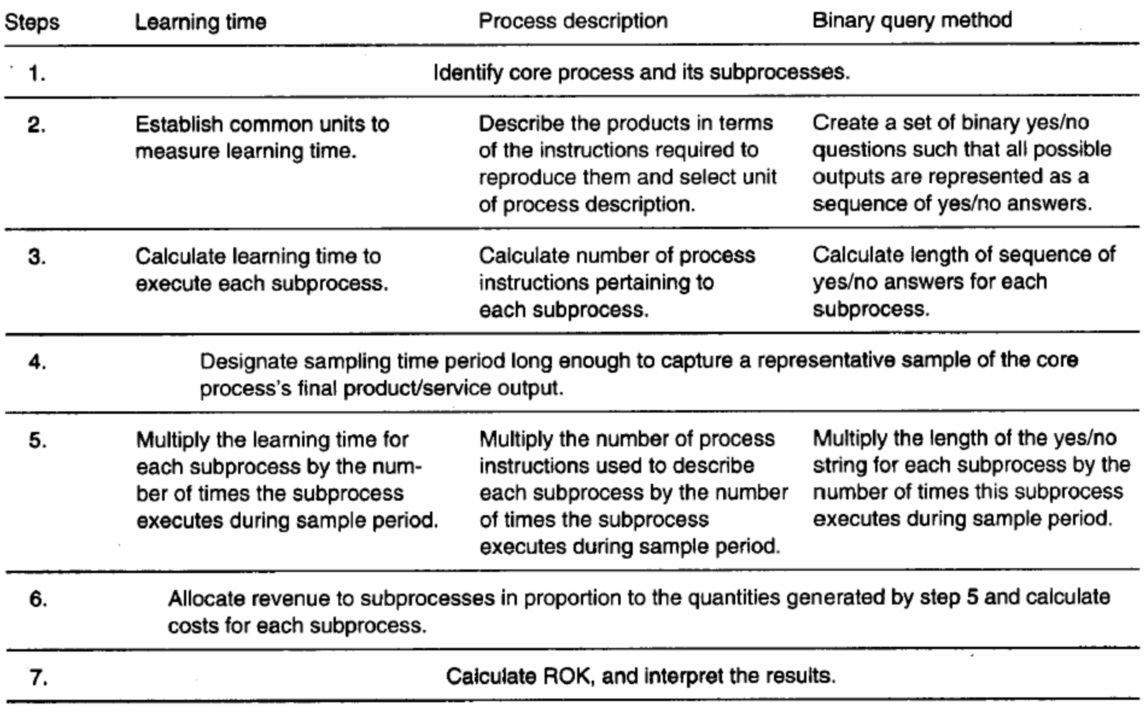
So "value" is proportional to "change" is proportional to "the amount of knowledge required to make the change"

Figure 5. Fundamental Assumptions of KVA (From: Housel and Bell, 2001)

The fundamental assumptions are where KVA derives its validity as a knowledge measurement method. It logically follows that if a process produces an output that is different from an input, then that change is proportional to the amount of value resident within the process, assuming the changes produce the correct output. If we have knowledge of the process that is necessary to produce the change, then we have the amount of change introduced by the knowledge (Housel and Bell, 2001). The resulting conclusion is that knowledge and change are proportional and can be used as surrogates for value when assessing process units of output. The utility to managers is that the output of all processes becomes standardized in terms of the units of knowledge required to produce it.

2. Approaches to KVA

What makes KVA an attractive approach is that the method is simple enough to be applied in seven steps yet it is robust enough to produce a desired level of granularity should managers desire a more comprehensive view of organizational processes. Housel and Bell (2001) offer three different ways to establish the value of knowledge embedded in the firm's core processes. Each is summarized in Table 3.

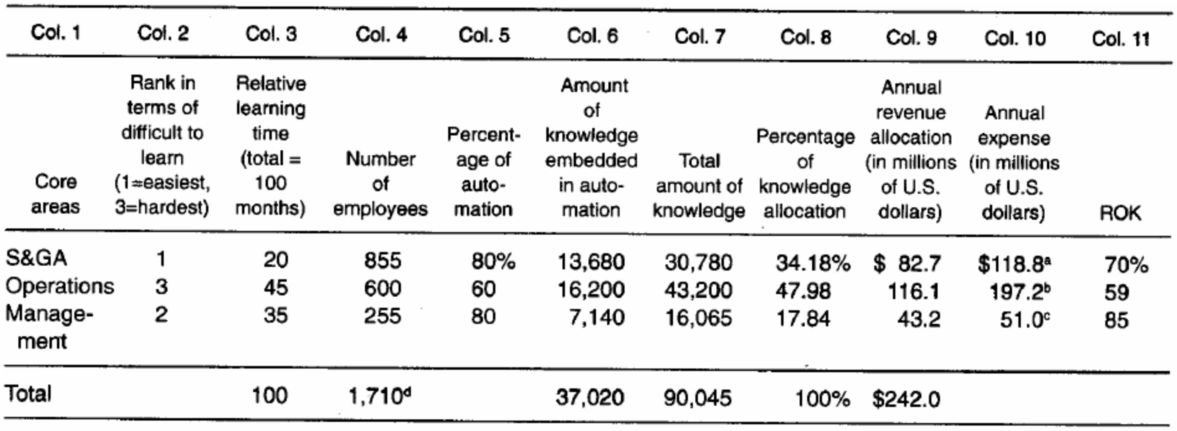


Steps	Learning time	Process description	Binary query method
1.	Identify core process and its subprocesses.		
2.	Establish common units to measure learning time.	Describe the products in terms of the instructions required to reproduce them and select unit of process description.	Create a set of binary yes/no questions such that all possible outputs are represented as a sequence of yes/no answers.
3.	Calculate learning time to execute each subprocess.	Calculate number of process instructions pertaining to each subprocess.	Calculate length of sequence of yes/no answers for each subprocess.
4.	Designate sampling time period long enough to capture a representative sample of the core process's final product/service output.		
5.	Multiply the learning time for each subprocess by the number of times the subprocess executes during sample period.	Multiply the number of process instructions used to describe each subprocess by the number of times the subprocess executes during sample period.	Multiply the length of the yes/no string for each subprocess by the number of times this subprocess executes during sample period.
6.	Allocate revenue to subprocesses in proportion to the quantities generated by step 5 and calculate costs for each subprocess.		
7.	Calculate ROK, and interpret the results.		

Table 3. Three Approaches to KVA (From Housel and Bell, 2001)

B. KVA METHOD

Although the binary query method is generally the most accurate, it is also the most time consuming and primarily reserved for situations requiring a high degree of accuracy and granularity. The method of analysis for our Proof of Concept is the Learning Time method. This method allows those who use it to establish rough-cut estimates of the value of knowledge within processes. It can be accomplished more quickly than the binary query method and is targeted at the aggregate level of analysis. An example of a high-level aggregate KVA analysis is shown in Table 4.



Col. 1	Col. 2	Col. 3	Col. 4	Col. 5	Col. 6	Col. 7	Col. 8	Col. 9	Col. 10	Col. 11
Core areas	Rank in terms of difficult to learn (1≈easiest, 3=hardest)	Relative learning time (total = 100 months)	Number of employees	Percent-age of auto-mation	Amount of knowledge embedded in auto-mation	Total amount of knowledge	Percentage of knowledge allocation	Annual revenue allocation (in millions of U.S. dollars)	Annual expense (in millions of U.S. dollars)	ROK
S&GA	1	20	855	80%	13,680	30,780	34.18%	$ 82.7	$118.8[a]	70%
Operations	3	45	600	60	16,200	43,200	47.98	116.1	197.2[b]	59
Manage-ment	2	35	255	80	7,140	16,065	17.84	43.2	51.0[c]	85
Total		100	1,710[d]		37,020	90,045	100%	$242.0		

Table 4. High-level Aggregate KVA Analysis (From Housel and Bell, 2001)

Table 4 shows the results of a seven step high-level KVA analysis of Exodus Communications[15] 1999 performance. Immediately, managers are able to see the relative performance of core functional areas in terms of ROK. The results serve as a launching point from which a more detailed KVA analysis can be done to identify knowledge deployed in sub-processes and to help managers make better decisions on how to make the company more profitable.

[15] Exodus Communications is an Internet data center company that was founded in 1994. The company offers system and network management solutions for customers' websites. (Housel and Bell, 2001)

1. Learning Time

Due to time constraints and limited access to CNVT personnel, it was determined that the Learning Time method would be used. In this method, the amount of knowledge embedded in a process is represented as the amount of time necessary for an average person to learn how to correctly execute that process. Since we are unable to compare results to those of the process description or binary query method, we used correlation between ordinal rankings, relative learn time (RLT) and actual learn time (ALT) to determine the reliability of the estimate. The three terms are described below:

- Ordinal Rank - is a measure of the firm's core processes in terms of difficulty to learn. Executives within the company are asked to rank core processes from hardest to easiest or most to least complex to learn (Housel and Bell, 2001).
- Relative Learn Time – a measure of the time it takes to learn each process relative to 100 months. Given 100 months total time to learn every core area, executives are asked to estimate how long it would take the average person to learn how to correctly execute each core process.
- Actual Learn Time – is an estimate of the real world learning time for the average person to learn each core processes. There are no limitations regarding total time allotted as in the RLT figure.

Using these values, the goal is to obtain a correlation figure of .8 or higher. A lesser figure would indicate that management is perhaps not using a common reference point for estimation and our estimates are therefore inaccurate (Housel and Bell, 2001).

The final part of the initial analysis is to get an accurate count of the number of times knowledge is executed during the sampling period and the time it takes to execute. These figures are representative of value and cost, respectively (International Engineering Consortium KVA tutorial). For our Proof of Concept, these figures are represented as "times fired", head count and work time (WT). To help ensure accuracy of knowledge estimates, it is important to note that two basic rules be followed. First, to avoid overestimation, knowledge should be counted only when in use[16]. Secondly, to obtain the output of a given process, always seek to find the shortest path description.

[16] Tutorial on Knowledge Value-Added Methodology. Web ProForum Tutorials. The International Engineering Consortium. (p. 6)

IV. DATA COLLECTION

This section provides the supporting research data for our POC and shows how we used the KVA methodology to capture the value added within a knowledge intensive process; specifically, our POC. The core processes involved in the planning and execution of a NCPAC CNVT network assessment will be examined, cradle to grave. This chapter discusses the rationale and explains the methods of gathering information and data used to develop and support this concept. The objective and scope of data collection are also addressed.

A. OBJECTIVE

Data collection is focused on obtaining appropriate information that will answer the research questions. Here we will explain how that data was collected. The valuation of the knowledge associated with the processes identified during our data collection will serve to identify opportunities for increased returns. The questions posed revolve around increasing the capacity of knowledge intensive processes. Capacity in this venue refers to allowing more room/time to provide more services to customers and stakeholders. This includes training for team members on new technologies, addressing high priority issues without largely impacting an existing schedule, or providing input for establishing network security/IA guidance and policies for the COCOM.

B. SCOPE

The Scope of our Data Collection efforts was limited to the CNVT Assessment Process. The actual assessment process exists to identify IA weaknesses and network vulnerabilities and help harden activities within the PACOM AOR against IA threats. Within DoD, assessment teams are assigned the missions of ensuring commands are compliant with IA security directives and that administrators are educated in maintaining secure, stable infrastructures[17]. When performing an assessment, team members use similar attack techniques and information gathering tools that attackers use to fingerprint and enumerate remote targets. Again, capabilities and thoroughness can be constrained by local command guidelines or real-world situational requirements.

[17] Title 10, United Stated Code, Section 224.

Assessments can be performed either internal or external to the network but the processes remain the same. The primary goal of an external assessment is to determine what sensitive information attackers might obtain by probing the network (Northcut, et al. 2003). An internal assessment looks at permissions and requires the administrators to test the configurations of perimeter components to verify security. Assessment personnel must keep pace with the fluid and knowledge intensive field of IA to ensure continuity of security. Although the scope of our data collection was focused on an IA assessment process, the concepts and lessons that can be drawn from our case are generic and can be applied to any knowledge intensive process.

C. COLLECTION METHODOLOGY

1. CNVT Process Audit

In our literature review, we concluded that process reengineering for a knowledge intensive organization could be accomplished by combining the fundamentals of Davenport and Short's five-step process with some of El Sawy's BPR principles. To begin the task of reengineering the CNVT's processes, we conducted interviews, traveled with the team during assessments to do process audits, and researched DoD policies and directives. The interviews and process audits served two purposes, which facilitated the completion of the first two steps of the five-step process; (1) to ensure we knew the CNVT concerns, and (2) to identify and validate existing processes. Members of the team repeatedly stated that their success was based on the quality of their product (assessment and guidance) and how they approached problems. They realized that they must maintain and keep track of automation advances in order to maintain a high level of knowledge (output to the customer). However, their operational tempo does not always allow for refreshment of knowledge. A recurring theme among the team members was that customer demand was increasing to the point that the team would not be able to provide service or an assessment.[18] From these concerns we were ultimately able to identify the need to increase CNVT process capacity and make better use of the limited knowledge assets inherent to the team as the objectives of this process redesign initiative.

[18] Meeting between PACOM CNVT and NPS team dated 29 August 2002.

Process audit data was collected during on-site assessments conducted in Korea and Hawaii. Both events proved extremely beneficial in identifying which processes were to be redesigned. We were able to see first hand, from the perspective of the CNVT member and the customer, where bottlenecks and inefficient practices hampered the network assessment process. By interviewing the Subject Matter Experts (SME's), CNVT members, and making observations, we were able to identify major processes and then break them down into sub processes where we identified respective inputs and outputs. Insight into augmentee contributions was observed as well, and interactions with clients were noted.

2. AS-IS Process

Information collected during interviews and observations during on site assessments enabled us to assess CNVT processes and build a model of the CNVT major processes. By interviewing the Subject Matter Experts, CNVT members, and making observations, we were able to recognize major processes and then break them down into sub processes where we identified respective inputs and outputs. The purpose was to establish the boundaries between processes and sub-processes and ultimately use the KVA methodology to identify and valuate the knowledge required for each. Our baseline "AS-IS" process model (Figure 6) was discovered to be relatively straightforward. The CNVT assessment process is comprised of the six core processes described below. Each core process requires a certain level of knowledge, and includes requirements for knowledge in IA, administration, and management. An interesting observation of their processes is that they lacked any notable usage of IT outside of the actual assessment process, other than normal office administrative functions such as email, word processing and spreadsheet usage.

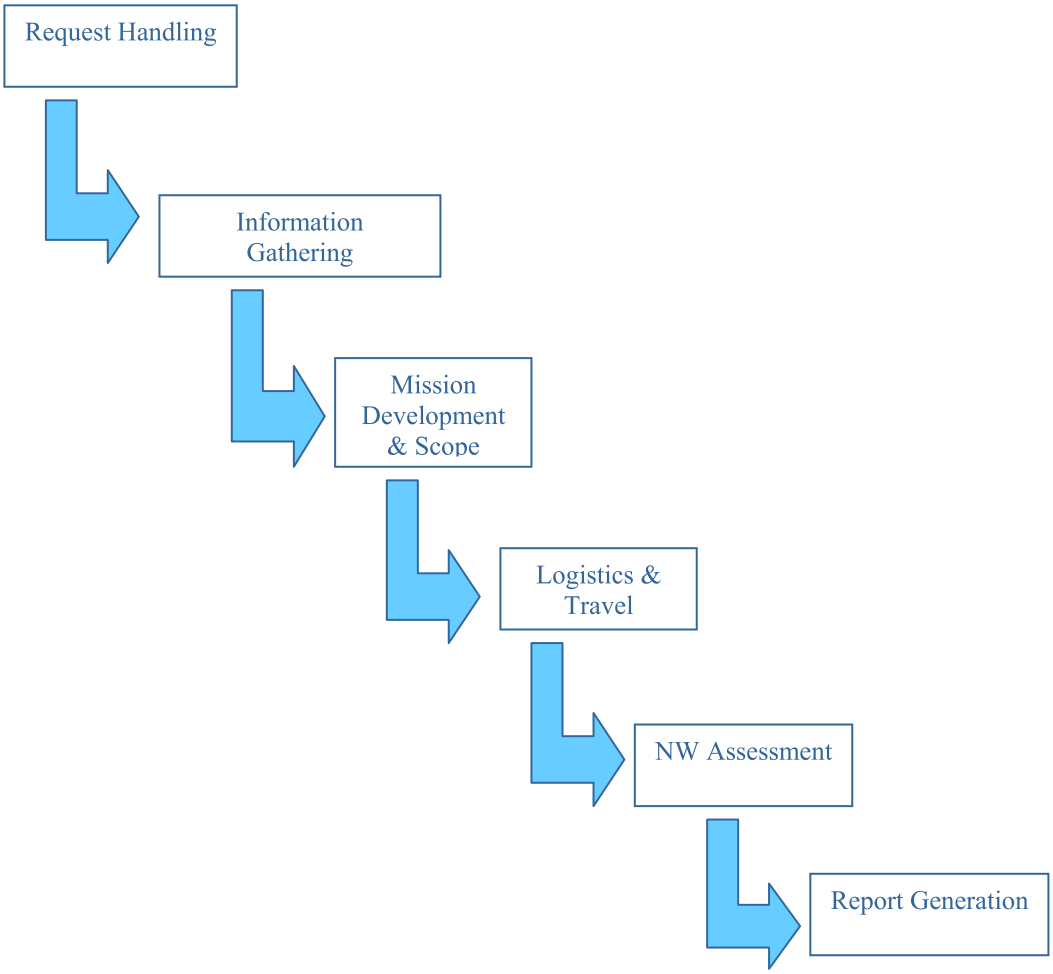


Figure 6. "As-Is" Process Model

a) Request Handling

In request handling, the call for customers goes out or calls for service are received and prioritized. Initial, very limited information about the customer is compiled and passed to the CNVT for their review. Legal Administration is also notified of a potential assessment. The purpose is to ensure that customers acknowledge CNVT assessment intrusion and provide protection for CNVT members should any legal issues arise. Sub-processes were identified as:

- Prioritize
- Request Report
- Compile Information
- Collaborate with CNVT

- Legal Administration

The request handling is largely managed by the PACOM, J39 (Information Operations Department). J39 prioritization is done based on PACOM goals, arising IA threats, and team availability[19]. This is the major point of entry for requesting an assessment.

b) Information Gathering

Information gathering is where the team sends out initial questionnaires and makes contact with potential commands to be assessed. Information concerning a command's network topology and infrastructure are requested and analyzed. Points of contact are also established and dialogues are created between customers and the team members. The CNVT questionnaire is attached as Appendix A. Sub-processes within information gathering were:

- Send Questionnaire or Survey
- Process Information

The use of e-mail, phone conversations, and facsimiles are the most common methods for conducting information gathering. Unless already stated, the goals of the assessment from the customer perspective are stated by the command and analyzed by the team.

c) Mission Development and Scope

The mission is developed from the preliminary information gathered from the customer combined with any specific COCOM IA goals. The preliminary information is taken, analyzed, and used to determine what expertise is required, help estimate the team size and requirement for augments[20], identify any particular hardware or software, and recognize any specific external resources that may be needed. The Sub-processes are:

- Funding
- Define Team Requirements
- Scoping
- Identification of augment requirements

[19] Phonecon between PACOM J39, CNVT members, and NPS Team members dated 7 October 2002.

[20] Augments to the CNVT include assets from the NSA C44 Network Security Evaluations and Tools Division, PACOM J65 Computer Network Defense/Information Assurance Division, and NPS Monterey.

- Legal approval

The determination as to whether or not an assessment can be done is based on inputs from Legal Administration and the availability of resources (funding or personnel). Legal issues may include a command conducting a classified exercise or a real world event[21]. Funds may not always be available and the command being assessed does not usually provide funding.

d) Logistics and Travel Planning

The trip planning and logistics of the mission are developed from the development and scoping of the mission. Travel arrangements include making reservations for vehicles, plane tickets, or hotels and ensuring travel orders are prepared and routed. Requests for Security clearance are generated and routed through the headquarters sections and out to the customer for concurrence. The logistics covers everything from ensuring augment orders are funded to making sure equipment is in line with the identified topology of the customer infrastructure. Sub-processes include:

- Ensure augments are identified
- Generation of travel orders
- Generation of and distribution of itinerary
- Points of Contact identified and contacted
- Any Legal issues resolved and completed
- Hardware prepared
- Security clearances completed
- Any special equipment identified and prepared to travel
- Customer network schematics and topology studied

Strategy meetings for each assessment are held to ensure responsibilities are known and understood. The mission lead is identified and any last minute details are addressed[22].

e) Network Assessment

The network assessment is the meat of the CNVT assessment process. It is here that the team interacts daily with and performs services for the customer. The

[21] During an assessment of the 516th Signal Brigade, UASRPAC, in Ft. Shafter, HI, the CNVT team and J65 personnel were restricted from doing any penetration testing due to circumstances surrounding Operations Iraqi Freedom and the War on Terrorism. USPACOM CNVT Assessment 3-11 April 2003.

[22] The team lead for the assessment at Ft. Shafter was a representative from the PACOM J6 Department.

team lead makes the major decisions from the beginning in-brief to the out-brief and consolidates recommended corrective action. The team responsibilities are distributed based on the structure of the network. Members are assigned areas of focus based on their expertise. For example, the member with network architecture expertise will be assigned the task of mapping the network and testing for vulnerabilities at the connection peripherals. Assessment Sub-processes are:

- In-Brief
- Equipment Set-up
- Assessment
- Out-Brief

The in-brief ranges from very formal to simple and informal and can address the entire staff or focus on the network personnel. Set-up and connection of equipment usually takes the better part of the first day. Access and permissions are enabled and passwords are assigned. The assessment portion is client dependent and is built around the goals of the mission as identified by the customer and considered by the team lead. The procedures are based on the team expertise present and are limited by any guidelines or restrictions placed on the team by the customer or higher headquarters. The usage of tools or particular methods is again expertise dependent.

The data is collected and a list of recommended corrective actions is generated. Various strengths and weaknesses are identified and documented. To conclude the assessment, an out-brief is given to highlight the most critical issues and provide positive feedback as well as identify areas to be improved with recommendations on how to effect changes. The data collected is consolidated and transported back to garrison with the team lead.

f) Report Generation

The final major process closes the cycle and provides captured data with interpretations to the customer. This data includes any discovered vulnerabilities, DoD directive or policy non-compliance, recommendations for corrective actions, team or command concern, and any positives noted. Sub-processes include:

- Compilation of output
- Review of the output and data analysis
- Recommendations and validation

- Actual consolidation of data and writing of the report
- Team concurrence
- Higher Headquarters approval for release
- Report sent to the assessed command

The report generation is completely centralized and managed from the team lead hands. Revisions are routed manually or via Secure Internet Protocol Routing Network (SIPRNET)[23] and include comments for augments as well as core team members. Actual delivery dates are dependent upon workload, operational tempo, and access to augmentees who may not be co-located. The final reports usually take 30-55 days before final delivery to customer is complete.

3. Ordinal Rankings

Having identified the core processes, we next compiled an ordinal ranking of the difficulty to learn each process. These are the subjective rankings of the processes ordered from what is perceived as least difficult (1) to most difficult (6) to learn. The ranking method serves as a baseline analysis that gives an initial perception as to which processes were least and most knowledge intensive. Each team member, including the J39 representative, was asked to rank the processes mentioned above. Table 5 shows the results:

Process:	**Ordinal Ranking**
Request Handling	1
Logistics	2
Information Gathering	3
Report Generation	4
Mission Development and Scope	5
Network Assessment	6

Table 5. Ordinal Rankings

[23] Although raw data may be unclassified, the consolidation of data may allow the construction of a command's network topology and identifies vulnerabilities that could serve as access points for attackers. Once consolidated, the information becomes classified.

The rankings serve as a benchmark that depicts the perceptions of the SME's as to which processes are the most demanding to accomplish.

4. Relative Learn Times

The relative learn time of a process is the amount to time it takes for an average person to learn how to do a process correctly. By documenting the relative learn times of each process, we get a common scale to measure against whether it is days, weeks, months, or years. Given 100 months, the SME's decide what time it would take to learn each respective process. The RLT's are cited in Table 6 below:

Process:	**Relative Learn Time (Hrs)**
Request Handling	5
Logistics	10
Information Gathering	10
Report Generation	20
Mission Development and Scope	25
Network Assessment	30

Table 6. Relative Learn Times

Intuitively, the process that is the most difficult should (and does) have the highest RLT.

5. Actual Learn Times

The ALT is the SME estimation on how long it actually took to learn a given process. We used hours for our unit of measurement. The ALT's are depicted in Table 7:

Process:	**ALT (HRS)**
Request Handling	8
Logistics	80
Information Gathering	8
Report Generation	32
Mission Development and Scope	120
Network Assessment	960

Table 7. Actual Learn Times

The Network Assessment has the highest ALT. In this case it correlates with having the highest RLT and being the most difficult process to learn based on the team member ordinal ranking.

6. Percent Information Technology

The percent IT represents the amount of IT that is used in each of the processes. Since interviews revealed that IT usage was minimal during the "administrative" type processes, we estimate that only a small portion of completing those particular processes is attributable to automation. For the remaining processes, significantly more IT is used and is reflected in the percent automation, as shown in Table 8:

Process:	**Percent Automation**
Request Handling	5
Logistics	5
Information Gathering	5
Report Generation	20
Mission Development and Scope	5
Network Assessment	75

Table 8. Percent Automation

The percent automaton estimates will be used in our KVA analysis to capture the value of knowledge that is deployed in IT. While it is intuitive that process completion depends heavily on the knowledge of the people executing it, if process completion also involves the use of IT, then a portion of the knowledge required to execute that process is in use within IT. Percent automation of IT allows us to capture those units of knowledge used in IT.

7. Cost Estimation

Cost estimation is the consolidation of Hourly cost for personnel and IT cost. Total cost is a summation of the two. The hourly cost is a rough estimation and is based on the average annual salary of a Department of Defense GS-14 employee. Since administrative uses of IT were deemed negligible, IT costs were estimated based on hardware and software costs that were CNVT specific. We estimated one fully configured laptop per team member (5 team members total) at an average cost of $2000 per laptop to yield a base cost of $10,000 per year. Spread across the CNVT average of 15 assessments per year yielded an average of $666 per visit. The individual IT costs for each process correlate to that percentage of usage as it relates to its process work time.

Process:	**Costs ($)**		
	Hourly	IT Cost	Total Cost
Request Handling	320	19	339
Logistics	7200	285	7485
Information Gathering	480	19	499
Report Generation	2880	114	2994
Mission Development and Scope	1600	38	1638
Network Assessment	8,000	190	8190

Table 9. Cost Estimations

8. Assumptions

Due to time limitations resulting in a short evaluation period and difficulties involved in coordination brought about by operational tempo, we were required to make several assumptions to enhance our understanding of the CNVT process. Assumptions are not preferred but the effects can be minimized as long as they remain consistent. Assumptions made were:

a) Incorporation of J39 Estimates

Since the J39 is most intimately familiar with the functions associated with the "Request Handling" process, we used their input for ALT, and WT for this process. The numbers differed somewhat from that of the CNVT members based on perspective. The J39 estimated ALT, and WT at 8, and 4 hours respectively. The team members valuated the same times at 4, and 2 hours respectively. The point of view is subjective and based on differences in perceptions between the entity that actually does the function and the personnel who merely observe and receive the output. ALT and WT estimations from the J39 were included to give us a more complete representation of the times involved in completing the assessment process. Our confidence in these estimations remains fairly high since the correlation[24] numbers did not substantially change when incorporating the J39 estimates (Table 10).

Correlation	Using CNVT Team Input:	Using J39 Input:
Rank to RLT	97.9 %	97.9 %
Rank to ALT	70.2 %	70.0 %
RLT to ALT	72.1 %	71.9 %

Table 10. Correlation of Estimates

b) CNVT Member Salary

The CNVT member salary input for Hourly cost was based on an estimated $40 per hour. This equates to the annual salary of a GS-14. The salaries were found to vary based on steps within the GS rating scale. However, since each team member performed every process, we kept the salary static. Benefits associated with DoD

[24] The level of correlation is an indication of the accuracy of the estimate (Housel and Bell, 2001).

employment (COLA, housing allowances, any travel pay, etc…) are not included since they are consistent and their inclusion would not affect the ROK relative final results.

c) License Fees

The CNVT receives application and software support from a variety of sources including NSA and the PACOM J6. As such, we assumed that any software licensing fees particular to CNVT missions was negligible. Additionally, many of the tools used by the team, such as L0phCrack, are free on the Internet. Software such as Solar Winds, NetIQ or ISS is provided from support activities or is also used outside of the specific CNVT mission. Finally, e-mail and any administrative tools are inherent to the cost of doing business as an entity within DoD and are not specific to the CNVT mission.

THIS PAGE INTENTIONALLY LEFT BLANK

V. DATA ANALYSIS

The purpose of this chapter is to summarize our analysis of the data collected to answer the research questions

A. "AS-IS" KVA ANALYSIS

Table 11 depicts a summary of a high level KVA analysis of CNVT's "as-is" processes. The entries of the table are summarized in the following paragraphs

Process	RLT	ALT	Work Time	Head Count	% Automation	Amount K in IT	Total K	% K Allocated	IT Cost	Total Cost	% C Allocated
Request Handling	5	8	4	2	5%	0.4	8.4	0.43%	$19	$339	1.60%
Logistics	10	80	60	3	5%	4	84	4.32%	$285	$7,485	35.40%
Information Gathering	10	8	4	3	5%	0.4.	8.4	0.43%	$19	$499	2.36%
Report generation	20	32	24	3	20%	6.4	38.4	1.97%	$114	$2,994	14.16%
Mission Development	25	120	8	5	5%	6	126	6.48%	$38	$1,638	7.75%
Network Assessment	30	960	40	5	75%	720	1680	86.37%	$190	$8,190	38.73%
Total	100	1208	140			737.2	1945	100.00%	$666	$21,146	100.00%

Table 11. High-level "As-Is" KVA Analysis

The core processes, RLT, ALT, Work Time and percent automation numbers were all obtained through data collection and described in the previous chapter. As such, their meanings will not be discussed further in this section. Rather than include a column for ordinal ranking, processes are listed in relative order of difficulty to learn.

1. Head Count

Head Count is representative of the number of people involved in completing a process. This number is an estimation based on interviews with CNVT members and others associated with the overall assessment process. Accounting for the number of employees gives a general idea of how often knowledge (K) is used and provides a rough-cut way of weighing the cost of using knowledge in the processes over the evaluation period (Housel and Bell, 2001).

2. Knowledge Allocation

In conducting a KVA analysis, if the degree of correlation between RLT and ALT is high enough, either estimate can be used in calculating ROK. For our POC case, we used the ALT estimate for our calculations. Since the units of knowledge in ALT are only fired once in completing a process, ALT is also representative of the amount of people knowledge (not depicted) used in each process. The amount of K in IT is determined by multiplying the amount of people K in each process by the percent attributable to automation. Therefore, total K is the summation of people K and amount of K in IT. This approach is used when the K in people and IT is not redundantly used to produce process outputs.

With total K calculated and represented as a common unit of measurement (based on 100 months relative learn time), a for-profit knowledge intensive organization would then be able to allocate revenue to each process based on the percentage of knowledge used in generating revenue. For DoD organizations, where knowledge execution does not result in generated revenue, knowledge allocation would give managers a better picture of where their most productive knowledge assets are deployed. While this doesn't give the complete picture of where the most "bang for the buck" is, it does provide us with the numerator of our overall return on knowledge equation.

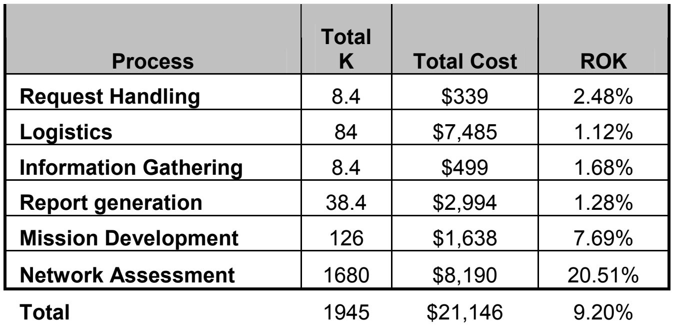
3. Cost Allocation

Hourly cost (depicted in Data Collection) is equal to the work time multiplied by the head count and the hourly salary for each employee. As previously discussed, hourly salary was roughly estimated at $40/hour and IT costs are based on an annualized cost of computer hardware for each CNVT member, with software costs being negligible. As in our calculations for total K, total cost is a summation of hourly cost and IT cost.

With total cost calculated, we are able to further allocate costs to each core process based on a percentage. The unique manner in which KVA identifies costs enables managers to separate human labor costs from those associated with IT. This provides useful insight in that they are able to see which processes consume the most resources (cost) and have the biggest impact on their overall bottom-line.

4. Return on Knowledge

Table 12 depicts the return on knowledge achieved in the CNVT core processes.



Process	Total K	Total Cost	ROK
Request Handling	8.4	$339	2.48%
Logistics	84	$7,485	1.12%
Information Gathering	8.4	$499	1.68%
Report generation	38.4	$2,994	1.28%
Mission Development	126	$1,638	7.69%
Network Assessment	1680	$8,190	20.51%
Total	1945	$21,146	9.20%

Table 12. “As-Is” Return on Knowledge

As can be immediately seen, the four processes that CNVT members deemed the easiest to learn in terms of relative difficulty are generating the least returns on knowledge. Request handling, logistics, information gathering and report generation all produce returns of less than 3% while the most return is realized in the network assessment process. At the aggregate level, the current processes only generate an ROK of 9.2%. The results are not surprising since CNVT members attribute a significantly larger portion of actual learn time to network assessment than the other processes. However, analysis of this table extends beyond the obvious ROK numbers. Costs of those processes generating little return should also be of equal importance to managers of knowledge intensive organizations and should prompt them to consider why a costly process generates such little return. Logistics, for example, is nearly as costly as the network assessment process, yet generates significantly less return on knowledge. On the converse, one might consider what enables a high cost process such as Network Assessment to generate such a high return.

5. Return on IT

Table 13 depicts the return on IT achieved in the CNVT core processes.

	Amount		
Process	K in IT	IT Cost	ROIT
Request Handling	0.4	$19	2.10%
Logistics	4	$285	1.40%
Information Gathering	0.4	$19	2.10%
Report generation	6.4	$114	5.61%
Mission Development	7	$38	15.77%
Network Assessment	720	$190	378.38%
Total	737.2	$666	110.69%

Table 13. Return on IT

Like return on knowledge, return on IT shows similar results. As expected, the processes which were automated the most show the most amount of knowledge in use within IT and, a priori, the most return on IT. Inferences to be drawn from this table are similar to those that were drawn from the ROK table.

B. REENGINEERING CORE PROCESSES

In considering the results of the KVA analysis of the "as-is" processes and the descriptions of core processes as defined by CNVT members, it becomes apparent that the organization is plagued with problems related to inefficient information flow and ineffective knowledge management. In particular, the most immediately recognizable problems are described below:

- Information flow about processes is rudimentary. From compiling the prioritization list for assessments to gathering information about customers, it seems as though the "stubby pencil" and sneaker-net techniques are the prevailing methods of communication.

- Indirect access to available knowledge. With exception of being mission leads, CNVT members have little direct access to information about the command being assessed until the mission planning starts

- Knowledge sharing coordination. Again, the sneaker-net prevails. There is no place for centralized collaboration among CNVT members and J39 representative. Furthermore, there is no centralized location for information to reside and enable visibility to all involved in the network assessment process. Other than face-to-face encounters, all parties involved, including the CNVT customers, must rely on email and phone calls as the primary means of coordination and collaboration.

Each of these problem areas contributes significantly to the relatively low returns on knowledge and IT highlighted in the KVA analysis. They are conducive to increased process completion times, which directly results in higher costs and decreased capacity. Even more critical, these problems highlight the fact that most knowledge deployed throughout CNVT's processes is resident within team member's heads and that there is no mechanism in place to facilitate knowledge capture to ensure it is retained as team members move on.

1. Principles and Tactics

To address the problems described above, we revisit the Leavitt diamond as our framework for process reengineering. Because CNVT is such a small organization, there is no doubt that by redesigning processes, the environment around the processes will need to be adjusted to maintain stability and balance. El Sawy (2001) identifies 10 principles and tactics for redesigning processes that are drawn from this framework. They are broken down into 3 different categories: Changing the configuration and structure of processes, changing the information flows around processes, and changing knowledge management around processes. In each category, we can identify one or two principles, which can assist in tackling redesigning the CNVT processes to address problem areas and ultimately increase process capacity. Those that are most applicable are described below.

For reconstructing and reconfiguring processes, principle #1 is to lose wait – squeezing out the wait time in a processes to increase value. From our initial data collection we saw that some of the processes involved rather large elapsed times because CNVT members were waiting for responses to emails and phone calls. Although elapsed time was not considered in our “as-is” KVA analysis, one can assume that a shorter elapsed time will directly translate to shorter work time since the process has become more streamlined.

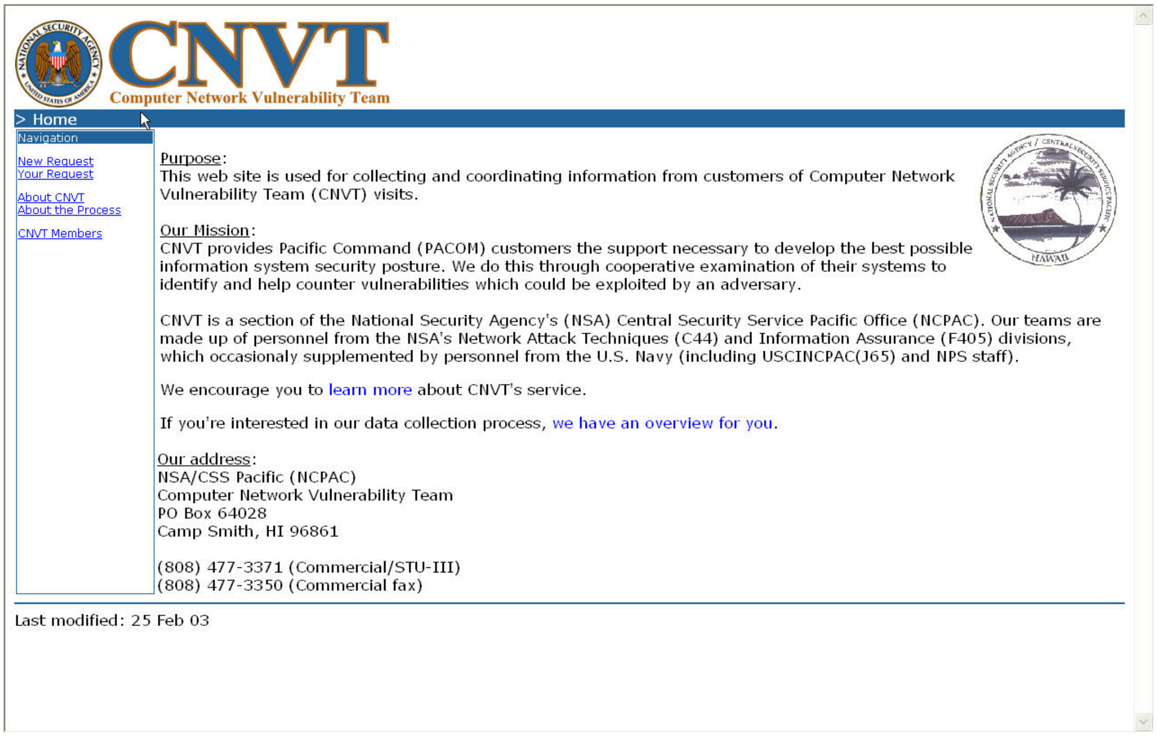
For changing information flows around the process there are two principles which can be applied. Principle 5 is to capture information digitally at the source and propagate it throughout the process. One way this can be accomplished is by web enabling as much of the process as possible and capturing information in a database. For example, information gathering can be web enabled to push the data entry to the customer rather than having the CNVT duplicate the effort when a survey is returned. Furthermore, the earlier you digitize the data, the more readily you can make it available for use throughout other processes. Principle 6 is to vitrify or provide glasslike visibility through fresher and richer information about a process. Both CNVT and the customer receive added value from increased visibility of information. For the CNVT, the value would be to know almost instantly where they stood in the planning stages of a network assessment. Customers receive value from being able to track the status of their request, similar to how FedEx generates value for its customers by allowing them to track the status of a shipment from the time it is picked up to when it is received. Also, since team members indicated a lot of elapsed time was attributable to trying to pull information from customers who were slow to complete the questionnaire, pushing the responsibility to the customer will prompt them to be more vigilant at providing more complete and timely information, especially since the status of their assessment depends on it.

For changing knowledge management around the process, principle 9 can be applied. Its intent is to connect, collect, and create. In other words grow intelligently reusable knowledge around the process through all who touch it. The principle can be encompassed through development of a repository of knowledge. Enabling the reuse of knowledge ensures that as team members gain more and more experience, the CNVT organization as a whole learns as well because knowledge is transferred to the repository. An example would be if a Windows expert discovers something (a new technique, or new remedy for a particular IA vulnerability), that knowledge is documented and stored in a repository for the next Windows expert to be able to use. This a key contribution to the overall value created because knowledge is no longer resident in the minds of team members and is able to be drawn from the repository at a relatively inexpensive cost.

2. Prototype

Having captured the value of knowledge deployed within CNVT processes and identified areas where process redesign and redeployment of knowledge can help increase process capacity, we developed a prototype that encompasses the principles of BPR previously discussed. This prototype addresses the recursive relationship between IT capabilities and BPR in that it incorporates the use of information technology to support redesigned processes rather than business functions. It also adheres to the two fundamental principles proposed by Housel and Bell (2001) of moving frequently deployed procedural knowledge to IT and capturing the knowledge that typically dies when an employee leaves. And although prototyping is the fifth and final stage of Davenport and Short's five-step process, it is important to keep in mind that design of the prototype does not signify the end; there will be successive iterations for further refinement and enhancing capabilities.

The designed prototype is a web-enabled database that facilitates capturing some of the tacit knowledge involved in the "administrative" core processes of a CNVT network assessment; request handling, information gathering, and mission planning. Because these processes generate the least amount of return on knowledge and IT, they are the focus of our efforts to more efficiently deploy knowledge and increase process capacity. The screen captures below illustrate the web pages of the prototype design.



Purpose:
This web site is used for collecting and coordinating information from customers of Computer Network Vulnerability Team (CNVT) visits.

Our Mission:
CNVT provides Pacific Command (PACOM) customers the support necessary to develop the best possible information system security posture. We do this through cooperative examination of their systems to identify and help counter vulnerabilities which could be exploited by an adversary.

CNVT is a section of the National Security Agency's (NSA) Central Security Service Pacific Office (NCPAC). Our teams are made up of personnel from the NSA's Network Attack Techniques (C44) and Information Assurance (F405) divisions, which occasionaly supplemented by personnel from the U.S. Navy (including USCINCPAC(J65) and NPS staff).

We encourage you to learn more about CNVT's service.

If you're interested in our data collection process, we have an overview for you.

Our address:
NSA/CSS Pacific (NCPAC)
Computer Network Vulnerability Team
PO Box 64028
Camp Smith, HI 96861

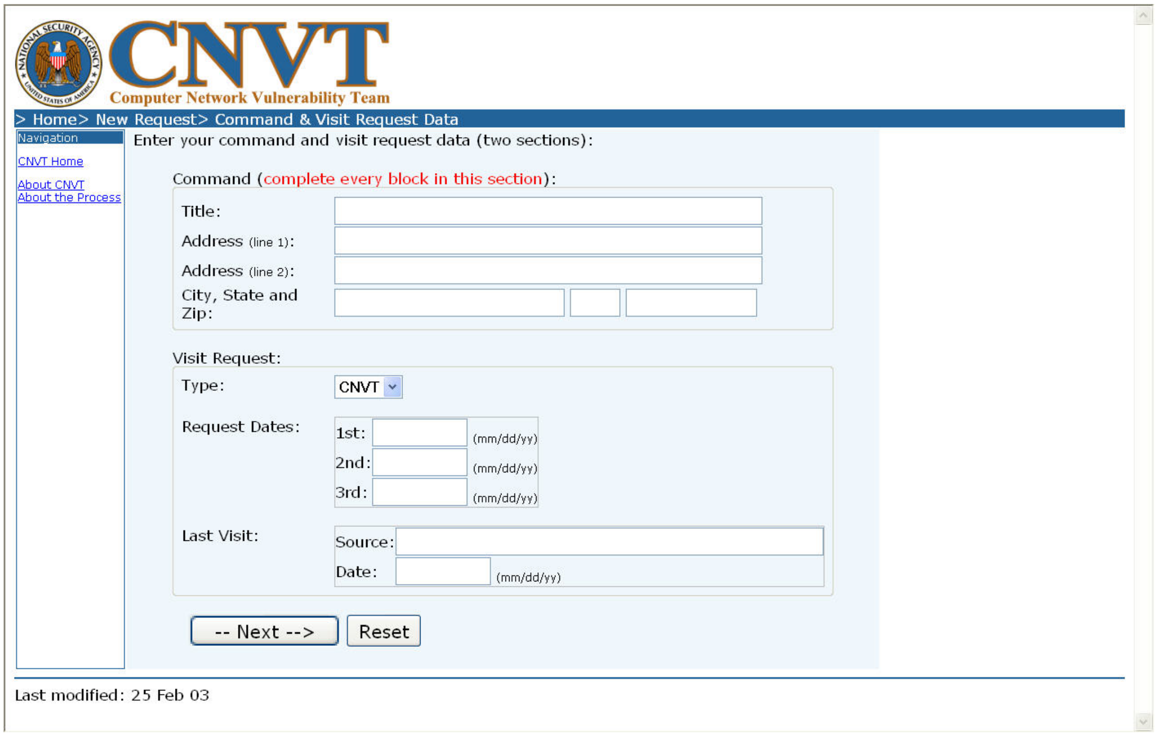
(808) 477-3371 (Commercial/STU-III)
(808) 477-3350 (Commercial fax)

Last modified: 25 Feb 03

Figure 7. Prototype Home Page

The homepage is the focal point of the prototype. It provides a general overview of the service provided by CNVT and serves as a launching point for navigation throughout the rest of the website. Navigation links are located on the left side of the page.

Clicking on the "New Request" link essentially walks the customers through a series of screens that digitally capture the information previously asked in the CNVT questionnaire. This is where the request for services is assigned a tracking number, enabling both CNVT and the customer to track the status at a later date.


CNVT
Computer Network Vulnerability Team
> Home> New Request> Command & Visit Request Data
Navigation
CNVT Home
About CNVT
About the Process
-- Next -->
Reset

Enter your command and visit request data (two sections):

Command (complete every block in this section):

Title:

Address (line 1):

Address (line 2):

City, State and Zip:

Visit Request:

Type: CNVT

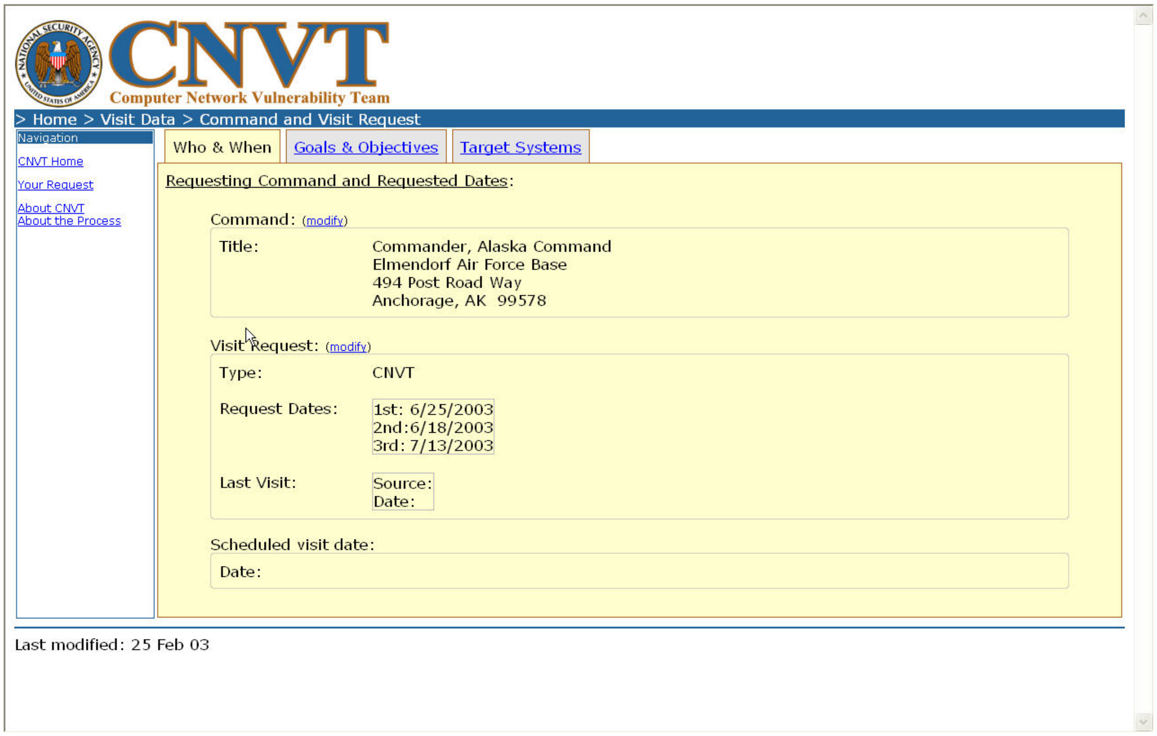
Request Dates:
1st: (mm/dd/yy)
2nd: (mm/dd/yy)
3rd: (mm/dd/yy)

Last Visit:
Source:
Date: (mm/dd/yy)

Last modified: 25 Feb 03

Figure 8. New Request Page

Figure 9 shows the summary of a sample request that was recalled by tracking number. Customers and CNVT members are able to modify, verify and add data to a particular request as more information becomes available by clicking on the subject tabs at the top of the page.



Requesting Command and Requested Dates:

Command:

Title: Commander, Alaska Command
Elmendorf Air Force Base
494 Post Road Way
Anchorage, AK 99578

Visit Request:

Type: CNVT

Request Dates: 1st: 6/25/2003
2nd:6/18/2003
3rd: 7/13/2003

Last Visit: Source:
Date:

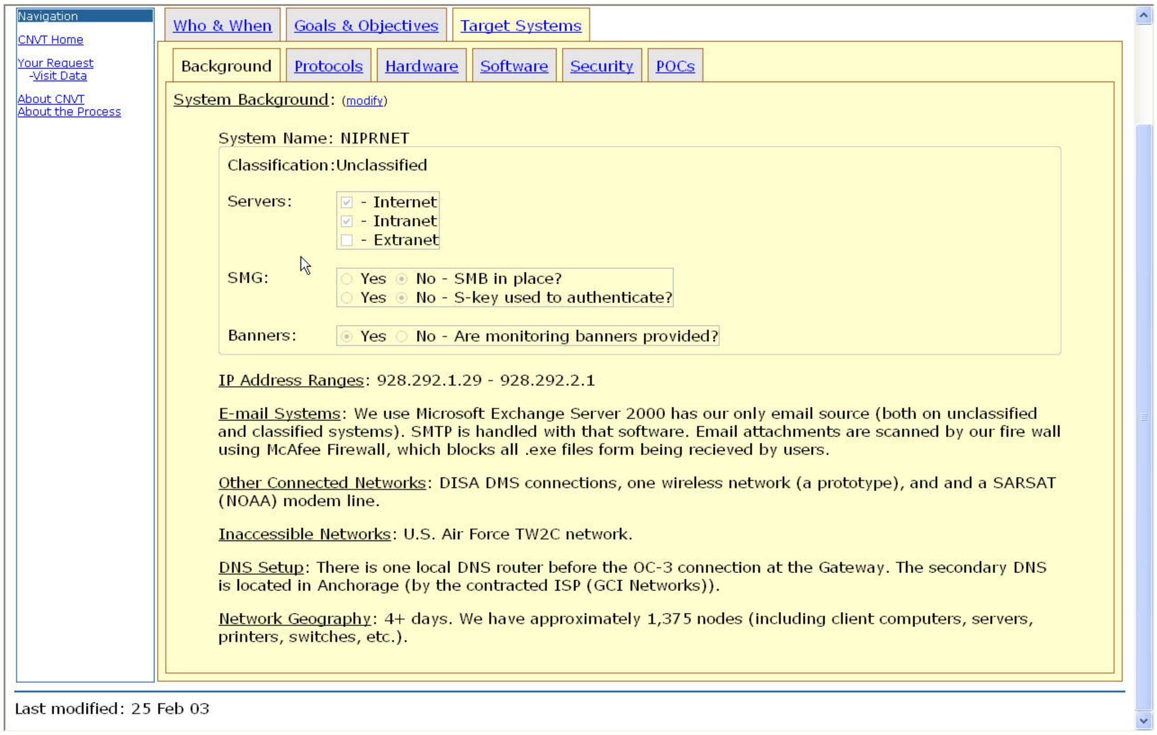
Scheduled visit date:

Date:

Last modified: 25 Feb 03

Figure 9. Summary of Request Page

Figure 10 depicts a summary of the network topology information as entered by the customer. When inputting the service request, customers are prompted for this information in the form of drop down menu, option boxes and text boxes. This enables CNVT to build a more complete picture of the network to be assessed by driving the customer to be very specific in the information they provide.



System Background: (modify)

System Name: NIPRNET

Classification:Unclassified

Servers: ☑ - Internet ☑ - Intranet □ - Extranet

SMG: ○ Yes ● No - SMB in place?
○ Yes ● No - S-key used to authenticate?

Banners: ● Yes ○ No - Are monitoring banners provided?

IP Address Ranges: 928.292.1.29 - 928.292.2.1

E-mail Systems: We use Microsoft Exchange Server 2000 has our only email source (both on unclassified and classified systems). SMTP is handled with that software. Email attachments are scanned by our fire wall using McAfee Firewall, which blocks all .exe files form being recieved by users.

Other Connected Networks: DISA DMS connections, one wireless network (a prototype), and and a SARSAT (NOAA) modem line.

Inaccessible Networks: U.S. Air Force TW2C network.

DNS Setup: There is one local DNS router before the OC-3 connection at the Gateway. The secondary DNS is located in Anchorage (by the contracted ISP (GCI Networks)).

Network Geography: 4+ days. We have approximately 1,375 nodes (including client computers, servers, printers, switches, etc.).

Last modified: 25 Feb 03

Figure 10. Network Summary Page

While not every page of the prototype is depicted here, they are attached as Appendix B. However, as indicated in the previous figures, the web enabled database is quite user friendly and allows us to accomplish several objectives that are beneficial to knowledge intensive organizations. From the customer perspective, the prototype enables them to more easily respond to the J39's annual call for services by submitting responses in the form of a request via the web site. Customers are also able to complete the CNVT assessment questionnaire and track the status of a request online.

The web site also serves as an information portal (linked to a database) for CNVT members and those associated with the network assessment core processes. By digitally capturing information early, visibility is increased and they are able to see the various bits of information provided by the customer throughout all stages of the assessment process.

Of value to both the CNVT and its customers is the unique ability to assign tracking numbers to requests when submitted. This allows customers, CNVT members, and the J39 representative the ability to track and monitor the status of a request from start to finish. Additionally, the request tracking number can be tied to specific task lists (checklists) for both the J39 and CNVT to facilitate process execution.

The prototype also provides a shared electronic database. Linked to the web-based input forms, this database would create shared access to information for CNVT members, the J39 and maybe even customers on a limited basis. Data could be tailored to exist as various forms and tables as dictated by CNVT needs. It can also be protected so that only pertinent information is made visible to appropriate personnel. An example would be an automatically generated list of all customers who have submitted a request in the past within a certain time period or a detailed listing of the findings from a previous assessment of a repeat customer. Such a database allows for the reuse of knowledge and fosters continual learning of the organization as well as individual team members.

3. Comparisons

Before entering into discussion of the example comparisons, it is important to qualify the utility of these calculations. Due to the small size of our proof of concept organization and limited sampling period within which we observed them, one cannot draw wide-ranging conclusions from these particular calculations. Furthermore, while not every network assessment is identical, the sampling period during which the CNVT was observed was assumed to be representative of the "average" network assessment. However, the concept behind the calculations and the approach to redesigning processes is general enough that the conclusions we draw from our POC can be applied to other knowledge intensive organizations.

The two tables below illustrate the KVA analysis of the "as-is" and "to-be" versions of the three administrative processes that we attempted to redesign with the prototype.

Process	RLT	ALT	Work Time	Head Count	% Automation	People K	Amount K in IT	Total K	Hourly Cost	IT Cost	Total Cost
Request Handling	5	8	4	2	5%	8	0.4	8.4	$320	$19	$339
Mission Development	25	120	8	5	5%	120	6	126	$1,600	$39	$1,639
Information Gathering	10	8	4	3	5%	8	0.4	8.4	$480	$19	$499
Total	40	136	16	10		136	6.8	142.8	$2,400	$77	$2,477

Table 14. High-level "As-IS" KVA Analysis of Three Processes

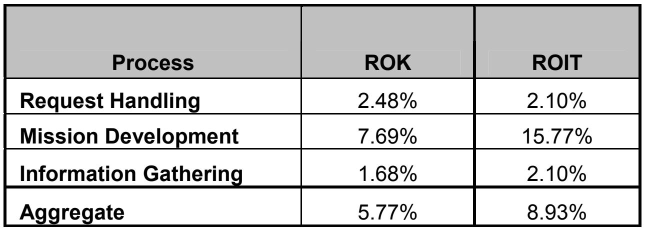
Process	RLT	ALT	Work Time	Head Count	% Automation	People K	Amount K in IT	Total K	Hourly Cost	IT Cost	Total Cost
Request Handling	5	8	2	2	70%	8	5.6	13.6	$160	$10	$170
Mission Development	25	120	4	2	20%	120	24	144	$320	$20	$340
Information Gathering	10	8	2	2	70%	8	5.6	13.6	$160	$10	$170
Total	40	136	8	6		136	35.2	171.2	$640	$40	$680

Table 15. High-level “To-Be” KVA Analysis of Three Processes

Based on interviews of CNVT members and their indicated likelihood of using such a system if fully implemented, we estimate significant increases in the percent automation of the three core processes analyzed. Additionally, we further assumed that, with increased collaboration and more readily available information, the amount of work time and head count required to complete each process would be reduced. These differences are reflected in the “to-be” KVA analysis.

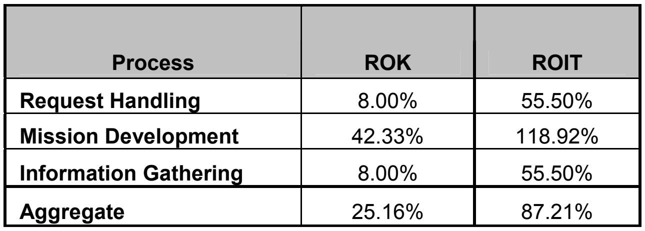
The tables reveal several interesting points worth noting. As suspected, with an increase in the use of IT and decrease in head count and work time, KVA shows us an overall decrease in total cost and increase in total knowledge executed in completing the processes. We attribute the decrease in total cost to two things. First, the reduced head count and work time reduces hourly cost – fewer employees working less hours equals less cost. Additionally, since IT costs are based an allocated percentage of total work time, the reduction in work time for the three processes results in decreased IT costs as well. The increase in total knowledge is attributed to the fact that increased automation now makes use of knowledge used in IT. As a result, the infusion of IT produces 28.4 more units of knowledge in addition to those units that exist in employees’ minds. These units of knowledge represent increased capacity that can be used elsewhere throughout the assessment.

Tables 16 and 17 depict a comparison of the “as-is” and “to-be” ROK and ROIT.



Process	ROK	ROIT
Request Handling	2.48%	2.10%
Mission Development	7.69%	15.77%
Information Gathering	1.68%	2.10%
Aggregate	5.77%	8.93%

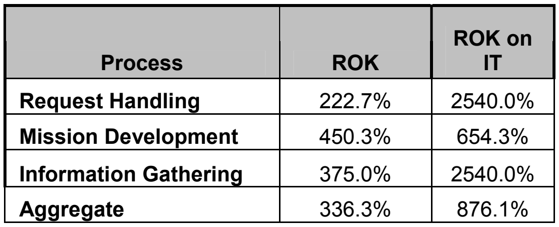
Table 16. “As-Is” ROK and ROIT



Process	ROK	ROIT
Request Handling	8.00%	55.50%
Mission Development	42.33%	118.92%
Information Gathering	8.00%	55.50%
Aggregate	25.16%	87.21%

Table 17. “To-Be” ROK and ROIT

As shown, use of a web-enabled database to facilitate completion of these three processes generates significant increases in the respective returns. As another point of reference, the percent increase in returns is shown in Table 18.



Process	ROK	ROK on IT
Request Handling	222.7%	2540.0%
Mission Development	450.3%	654.3%
Information Gathering	375.0%	2540.0%
Aggregate	336.3%	876.1%

Table 18. Percent Increase in ROK and ROIT

To further illustrate how the use of IT has impacted the assessment process overall, Table 19 shows a high-level aggregate KVA analysis of the “to-be” processes.

Process	RLT	ALT	Work Time	Head Count	% Automation	Amount K in IT	Total K	% K Allocated	IT Cost	Total Cost	% C Allocated
Request Handling	5	8	2	2	70%	5.6	13.6	0.69%	$10	$170	.88%
Logistics	10	80	60	3	5%	4	84	4.26%	$303	$7,503	38.70%
Information Gathering	10	8	2	2	70%	5.6	13.6	0.69%	$10	$170	.88%
Report generation	20	32	24	3	20%	6.4	38.4	1.95%	$121	$3,001	15.48%
Mission Development	25	120	4	2	20%	24	144	7.30%	$20	$340	1.75%
Network Assessment	30	960	40	5	75%	720	1680	85.12%	$202	$8,202	42.31%
Total	100	1208	132			765.6	1974	100.00%	$666	$19,386	100.00%

Table 19. High-level "To-Be" KVA Analysis

An important observation to note is that, while the IT costs changed for the three processes redesigned, the aggregate IT cost remains the same based on the assumption that our baseline cost for equipment is $666 per assessment and that the prototype can be developed in-house. The result is a cost reduction of $1760 per assessment. With an average of 15 assessments per year, this amounts to an annual savings of $26,400.

Process	Total K	Total Cost	ROK
Request Handling	13.6	$170	8.00%
Logistics	84	$7,503	1.12%
Information Gathering	13.6	$170	8.00%
Report generation	38.4	$3,001	1.28%
Mission Development	144	$340	42.33%
Network Assessment	1680	$8,202	20.48%
Total	1974	$19,386	10.18%

Table 20. "To-Be" Return on Knowledge

Overall ROK for the six core processes is shown in Table 20. The slight decrease in the Network Assessment ROK is due to the IT cost for that process increasing slightly as it is reallocated based on changes in process work times. When viewed at the aggregate level, we see that ROK overall is only increased to 10.18% from the 9.20% obtained in the "as-is". While this is appears to be a fairly insignificant increase, it is important to keep in mind that only the three lowest cost processes were redesigned in the POC case. In reengineering those processes within the constraints of this thesis, aggregate

ROK for those processes was increased to 25.16% from 5.77%, an overall increase of 336.3%. Additionally, the overall aggregate change in ROK, although small, represents a 10.7% increase achieved in a short time period.

C. SUMMARY OF ANALYSIS

The analysis performed on the data collected leads to the overall conclusion that IT can be used effectively to increase the process capacity of a knowledge intensive organization. The incorporation of Information Technology into existing processes, in particular, those "as-is" processes generating returns on knowledge of less than 3 percent, provides a substantial increase in returns on knowledge and IT. Replacing "stubby pencil" or "sneaker-net" methods with, for example, web interfaces and collaborative environments not only reduced process execution times, but also yielded a 336% increase in ROK.

To establish a reference for increase in process capacity, we make the assumption that the CNVT will continue to be funded at their current level of 15 network assessments per year. At an "as-is" cost of $21,146 per assessment, this equates to an annual cost of $317,190. Based on a predicted savings of $1,760 per assessment at a cost of $19,386, CNVT will be able to complete a total of 16.4 assessments annually given their current funding level. In addition to an increase in assessment capacity, a summation of man hours (work time x head count) for the "as-is" and "to-be" shows 512 and 468 man hours, respectively. This illustrates that implementation of a simple IT solution results in a reduction of 44 man hours per assessment or 660 man hours per year.

Although "webification" and automation is not true BPR according to Hammer, our KVA analysis clearly shows that a small infusion of a web interface for customers to input requests and to develop the initial topology produces immense returns. Through the use of a web-enabled database, processes capacity is increased by 10% while fewer people are required to complete processes. In an organization such as CNVT and others throughout DoD, this is extremely beneficial. Unlike most for-profit organizations, where fewer bodies equals less costs and more return on investment, in our proof of concept, fewer bodies required for each process means they are now more available to complete other processes, increasing their process capacity overall and return potential.

VI. DISCUSSION

A. RESEARCH QUESTION SUMMARY

The results of this study can best be described by addressing each specific research question.

1. Increasing Capacity

Can the capacity of knowledge intensive processes be increased using BPR and Knowledge Management principles? Though our literature review revealed a number of ways to increase the capacity of knowledge intensive processes, this thesis demonstrated that the capacity of knowledge intensive processes could be increased through application of existing principles and methodologies. El Sawy (2001) mentions that there must be a catalyst that brings about the recognition that change is required. In the case of the CNVT, the recognition that they needed increased process capacity served as the trigger. Whatever the catalyst is in any organization, however, the trigger that prompts change should lead to a decision to reengineer existing processes.

To increase process capacity through process reengineering, organizations must also identify the framework within which their processes are executed. In this thesis, fundamentals of BPR were explained which helped establish a framework from which our case could be evaluated. This framework, El Sawy's e-business speed loop (Figure 4), accurately depicts the environment in which our proof of concept and other knowledge intensive organizations must operate. Also, corporations have to discover methods of identifying the knowledge associated with core processes and then find a method of objectively measuring the knowledge associated with each process. For our purposes, the Knowledge Value Added Methodology fulfilled the requirement to capture and value knowledge associated with CNVT's processes.

With the e-business speed loop framework in mind, a process audit was conducted and, through the use of KVA, we were able to effectively measure the value of knowledge deployed within core processes and identify areas in which reengineering efforts should be focused. A summary of the knowledge measurement is depicted in Table 11. It shows which of the core processes were generating little return and which were creating the most value for the CNVT. The results served as a guide as to which processes our BPR efforts should be focused.

Applying some of the principles identified by Davenport and Short and El Sawy, a prototype was developed using IT as a key enabler to more efficient processes. The results of our analysis are shown in Tables 14-20. They reveal that, through a simple infusion of IT to automate some of the organization’s most administrative core processes, process capacity could be increased as knowledge is redeployed through IT. The organization benefits from a significant increase in return on knowledge and IT while both process work time, and the head count required to execute the process, are reduced, thus facilitating the availability of workers to execute more processes. Additionally, our results show that while process capacity is increased, the reduced head count translates to an extra 44 man hours per assessment available that can be used for further enhancement of knowledge or in execution of other processes.

2. Objective Measurement of the Value of Knowledge

Is there a way to objectively measure the value of knowledge deployed within knowledge-intensive processes? As mentioned in the literature review, the KVA methodology was chosen over others because it offered the capability to objectively measure the value of knowledge across an entire organization. In application of the KVA methodology to this case, it was again proven to be effective at objectively measuring the value of knowledge. Though the KVA methodology was used in over 100 other cases, this thesis was a test of using the methodology to measure the value of knowledge deployed within knowledge-intensive processes in the information assurance context. Using knowledge as a surrogate for the value associated with each process, we are able to quantitatively measure the input knowledge required for a process to complete without having to establish a link to an amount of revenue that was generated in executing processes. Through KVA, the focus remained on deployed knowledge and, as a result, comparisons could be made of very different activities and processes using a common frame of reference.

3. Automation of Processes

Can repeatable processes be automated or outsourced to increase the capacity of the CNVT? This thesis adequately demonstrates that repeatable processes can be automated to increase the capacity of the CNVT assessment process. Through the effective redeployment of knowledge in IT, automation of several core processes resulted in decreased process completion time and fewer people required to execute each process. Although BPR is much more than "Web-enabling" (El Sawy, 2001, p.7), the incorporation of a rudimentary web portal that captured the most administrative intensive processes yielded an aggregate ROK of 25.16% and ROIT of 87.21% compared to 5.77% and 8.93%, respectively, in the "as-is" process. This amounts to increases of 336.3% and 876.1%, respectively.

Because of the vast complexities involved in effectively evaluating and selecting an organization for outsourcing within the guidelines of DoD's numerous policies governing acquisition and Information Assurance, this research did not explore the feasibility of outsourcing CNVT functions.

4. Limitations

As previously mentioned, the scope of this thesis was limited to a small organization and a relatively short time period. This, combined with limited access to personnel, did not allow for a total redesign of CNVT's core processes. As Hammer (1990) points out, the ultimate purpose of reengineering through IT is to enable new processes rather than simply automating the existing ones. However, as Davenport and Short (1990) state, process redesign is an iterative process and does not end with the prototype. In the case of the CNVT, process automation as the first iteration was the only achievable goal given the constraints within which this thesis was conducted. Based on our observations, the current assessment process is effective but by no means efficient and has little room for capacity increase without the use of IT. Knowledge-rich assets are used to execute logistics and travel planning processes, handle their own administration and could be better used in completing other tasks. IT uses outside the normal e-mail or other daily business usage, is limited and lacking in all processes except the actual network assessment. To address these issues, future iterations can include a myriad of refinements to the prototype to further increase process capacity and aid in more efficient use of knowledge. Such enhancements include but are not limited to:

- A tie-in to the existing office management software. Other than meeting with the team leader, the J39 representative has limited visibility into the schedules of team members. Such a tie-in could generate a self-updating calendar that is refreshed as team members annotate their availability.
- Automatic reminders. As requests are submitted, the new system could generate a series of emails or reminders of tasks to be completed based on a predefined checklist established by CNVT.
- File sharing for increased collaboration. Similar to the technology developed by Groove Networks[25], a further enhancement could be a module that facilitates file sharing in a common virtual workspace. As suspected and confirmed in the three administrative processes previously addressed, the use of IT to enable file sharing in the report generation process is likely to produce similar reductions in cost and increases in returns on knowledge and IT
- A repository of knowledge. The database could be developed to allow storage of files from previous assessments. Whether it is in the form of an actual assessment report or simply a tips or lessons learned document from previous trips, such a small knowledge intensive organization will see significant value from the use of reusable knowledge.
- Visibility beyond CNVT, customers and J39. Such a system should include visibility to all those who touch and impact CNVT's core processes. An example would be including a tie-in to Legal to aid in completion of that portion of the process.
-

[25] Groove Networks is a privately held company founded in 1997. Based in Beverly, MA, the company provides desktop collaboration software aimed at accelerating business activity within and across organizational boundaries. More information can be found at http://www.groove.net

B. RECOMMENDATIONS

The benefits of this research span the entire spectrum of knowledge intensive processes. The ideals and data presented further confirm that the KVA methodology and BPR are suitable for increasing value within processes.

1. CNVT Specific

In the context of this research, the CNVT is a knowledge intensive organization that can benefit from application of the principles and methodology discussed in this thesis. In general, process capacity can be increased, however closer examination of the CNVT reveals potential opportunities to improve performance overall to help meet team objectives.

a) Automate

Though not all agree that automation is the best approach to redesigning process, this thesis shows that, through proper use of IT as an enabler, automating basic processes can yield substantial returns on knowledge and ultimately increase process capacity. While the scope of our BPR efforts were only focused on three of CNVT's most administrative processes, KVA analysis showed that other process could be improved as well. CNVT should consider further development of the designed prototype to include addressing the limitations previously discussed and further expansion to incorporate all of its core processes.

Although contracting this requirement to an outside source is a viable option, the Naval Postgraduate School (NPS) provides a cost effective resource of talent that can be used to further enhance the capabilities of the prototype. CNVT should seriously consider NPS and its pool of thesis students as an option for future prototype development.

b) Advocacy

Our interviews and research revealed that CNVT could further benefit from more advocacy within the National Security Agency (NSA), their parent organization. Although successful at meeting the obligations and fulfilling the current goals of the PACOM Combatant Commander, all indications are that demand for their services within PACOM's AOR will continue to increase, thus the need for increased process capacity. This thesis has shown that increased capacity can be achieved though application of BPR principles and the use of IT. However, their increased potential will not be fully realized unless they are funded to support more than the current 10 to 15 missions per year. This will require more support from within PACOM and from their parent organization.

c) Administration of Tasks

The current method of obtaining information about customer networks to be assessed requires CNVT members to actively participate in establishing points of contact with the customer and "pulling" information from them. While the prototype shifts the information gathering to more of a "pull" type environment, until fully implemented, CNVT members will still have to liaison with the customer prior to executing a mission. The use of CNVT personnel to liaison with customers and accomplish other logistical tasks such as travel planning and basic administrative duties is an extremely inefficient use of knowledge-rich assets, as indicated by the low ROK's generated. An effective remedy would be to establish an administrative assistant to serve as a single point of contact for all liaisons with CNVT customers and absorb the responsibility of executing the remaining administrative type processes. Establishing such a position facilitates a more effective means of communication since all information about customers will flow through one person. In addition, team members' time can more effectively be used to conduct training or tend to other matters that enhance their knowledge.

d) Train

This thesis clearly illustrates that CNVT process capacity can be increased. However, the increased potential can not be fully realized until the decision is made to act on the information provided. It is simple to infuse the IT solution yet regress by continuing to produce the same amount of assessments by taking longer to execute processes since the extra time is available. A much more challenging and beneficial task, however, is to utilize the extra capacity and available man hours in developing a training regimen to further enhance team members' knowledge. With the steady proliferation of new technology such as wireless capabilities throughout DoD's networks, CNVT would surely benefit from using enhancing their knowledge of these areas to better prepare them for future network assessments.

2. General

a) Champion of Change

Within the proof of concept used in this thesis, it was clearly evident that the focus organization was committed to making a change. However, in organizations where personnel are firmly entrenched on conducting business processes a certain way, effecting even the slightest incremental change might not be an easy task. As the literature review revealed, the most common cause of BPR failure is lack of sustained commitment from management and leadership. In most redesign efforts, there will undoubtedly be resistance to change from within, as the "rice bowl"[26] effect tends to shape attitudes towards change. Such resistance can be overcome, however, if there are champions of change within the organization who effectively communicate and embody what the change is about.

b) Self Evaluate

Throughout any knowledge intensive organization, the need to continually self-evaluate cannot be underscored enough. In today's global economy, the environments in which organizations have established strongholds are constantly changing. As a result, the means by which a firm maintains its stronghold must continually change as well. Self-evaluation provides a means for companies to assess processes and identify areas that can be approved. This self-assessment should be focused on identifying which processes are creating the most value for the company and which are generating the least amount of return. For knowledge intensive organizations, the focus should be identifying means of efficiently deploying knowledge assets to ensure they are utilized to maximum capacity. This thesis identified a method that allows organizations to accomplish this. However, not every organization is ripe for a BPR project. Where total process redesign is not an option, simply identifying a means to streamline a single process through more efficient knowledge deployment, rather than

[26] The "rice bowl" effect refers to the belief that as elements of change are introduced, the power and authority of an individual or organization is reduced, resulting in increased resistance to implementation by that individual or organization.

redesigning it all together, is likely to yield significant improvements in ROK. As such, companies should always self evaluate to determine where value creation could be improved through redeployment of knowledge.

APPENDIX A. SAMPLE OPERATIONAL EVALUATION QUESTIONNAIRE

In order to scope the effort involved for the operational evaluation, CNVT asks questions that are typical of any computer network assessment. For classification purposes, the actual CNVT operational evaluation questionnaire was excluded to keep this thesis unclassified. In lieu of the CNVT questionnaire, a similar self assessment questionnaire is included. Although much broader in scope, this questionnaire adequately reflects the nature of questions asked by CNVT.

Management
==========

1. Has senior management, including the corporate or organizational
board of directors, established an appropriate information and
Internet security policy and an auditing process?

2. Is security viewed as an overhead activity or essential to business
survivability? Are security considerations a routine part of your
normal business processes?

3. Are there legal or regulatory requirements that you should be complying
with because of either contract commitments or the industry
sector in which you operate?

4. Do managers at each level of the organization understand their roles
and responsibilities with respect to information security? How do you
verify that? Do you understand your role?

Policy
======

5. What are your organization's most important security policies and
what business objectives do they help satisfy?

6. What is your role in ensuring that security policies are followed?

7. What are the consequences for non-compliance?

8. Is there potential liability for not exercising an appropriate standard
of due care?

9. If you are a publicly traded company and conduct business on the Internet, are risks to e-commerce revenues reported in annual reports?

Risk
====

10. How does your organization identify critical information assets and risks to those assets?

11. Are there any critical assets for which you are responsible?

12. Is the frequency and scope of your risk evaluation sufficient to take evolving threats into account?

13. Are risks to critical assets managed in a similar fashion to other key business risks? Are all critical assets reviewed in an annualexternal audit?

14. What are the potential financial impacts of a successful attack against these assets?

15. Do you have adequate insurance policies?

Security, Architecture and Design
=================================

16. What are the primary components of your organization's security architecture? Does your due diligence and due care process include reviews of outsourced resources?

17. What business objectives does your security architecture help satisfy?

18. Do you have a process to determine the security impact of linking new systems to your enterprise-wide architecture?

19. What assets are most securely protected and why? What are the five most critical business functions that depend on these assets?

20. If you don't know, whom do you ask?

Accountability and Training
===========================

21. When was the last time you and other senior managers, including your board, received a briefing or attended user training on information security as practiced in your organization?

22. Is your corporate audit function included in security policy and practices reviews? Is there an auditable process with defined exception policies to limit the corporation's liability if an employee

uses computing resources for malicious or illegal purposes?

23. What are your responsibilities to ensure that these practices are followed?

User Issues
========

24. When was the last time you and other senior managers, including your board, received a briefing or attended user training on information security as practiced in your organization?

25. Is your corporate audit function included in security policy and practices reviews? Is there an auditable process with defined exception policies to limit the corporation's liability if an employee uses computing resources for malicious or illegal purposes?

26. What are your responsibilities to ensure that these practices are followed?

Access Control
==============

27. How do you ensure that each employee only has access to the files, directories, and applications commensurate with their job responsibilities and their need to know? How often are permissions reviewed for appropriateness and accuracy?

28. How do you create a public/private key pair to encrypt sensitive information?

29. How do you share your public key with others and how do they share their keys with you?

Software Integrity
=================

30. What is the responsibility of users, including senior management, to safely operate systems?

31. How often do you scan for viruses on your desktop and laptop systems?

32. What actions do you take if you discover a virus?

33. How do you recover compromised files?

34 How do you contain the damage caused by a virus?

35. How do you avoid propagating a virus to others?

36. How do you verify that a recently created file has not been tampered with?

37. Do your administrators regularly scan for the presence of viruses, worms, Trojan horses, and denial-of-service agents?

Backup
======

38. What do you do when you want to retrieve a backup file that you inadvertently deleted? How long does this take?

39. What is your role in backing up the user data on your desktop and laptop?

Authentication and Authorization of Users
===

40. What means of identification and authentication do you need for accessing the systems you use every day? For accessing critical, more highly protected systems that you may need to use from time to time?

41. How do you access your organization's network and systems when you are working from home or when traveling? Are you allowed to dial directly into modems attached to desktops or servers?

42. Is your access restricted compared to what you can do when you are in the office?

43. Do you have decision processes and supporting procedures in place to permit third party access, manage each type of relationship with the appropriate level of security, and retire or update accounts when partnerships terminate?

44. If you don't know, whom do you ask?

Monitor and Alert
=================

45. When something doesn't look quite right on your system, whom do you call and what information do you need to provide to describe the problem?

46. Have your systems ever been compromised? How do you know?

47. Whom do you call to find out how your email and Web access are

being monitored?

48. Do your system and network administrators have an active contact list of peers for the primary networks with which yours interface?

49. Are your administrators up to date on the latest threats, attacks, and solutions? What resources do they use?

Physical Security
=================

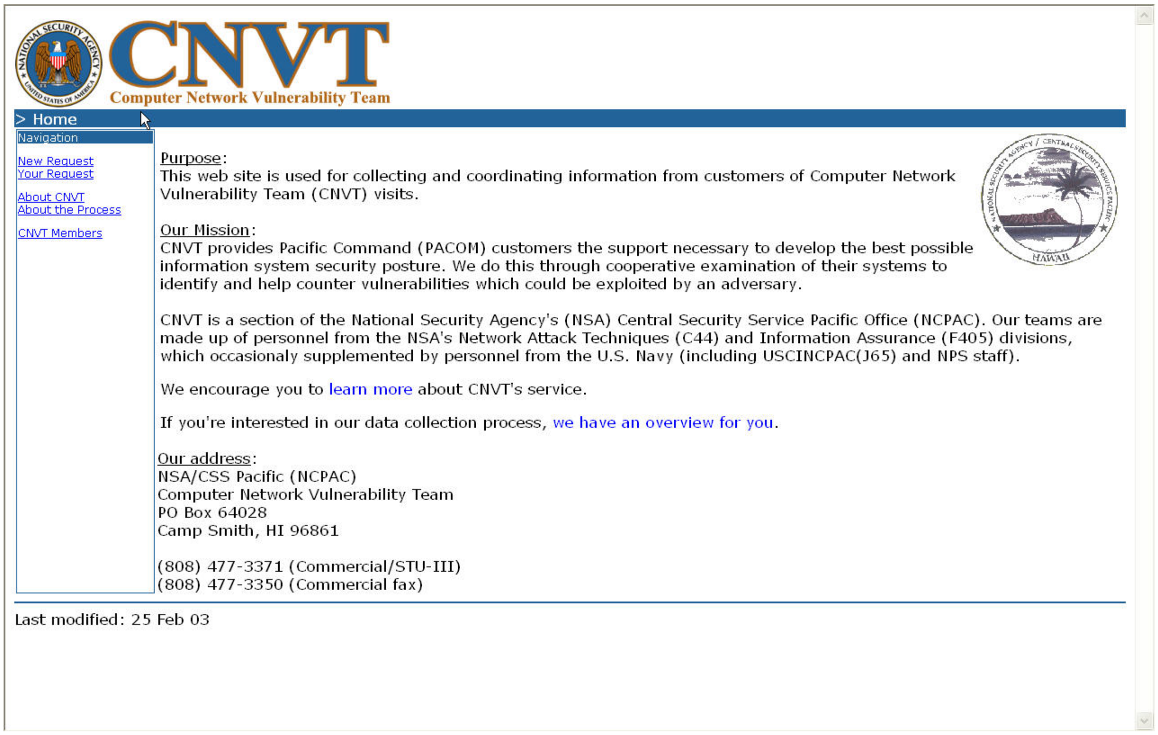
50. What means of identification and authentication do you need for accessing the primary facility where your office is? Critical facilities that you are required to visit from time to time?

51. What assurances do you have that physical security access restrictions are being followed? How are violations reported to you?

52. Do you know whom to contact if you detect suspicious letters, packages, or other items sent by mail or a delivery service? What is considered suspicious?

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B PROTOTYPE WEBSITE



Purpose:
This web site is used for collecting and coordinating information from customers of Computer Network Vulnerability Team (CNVT) visits.

Our Mission:
CNVT provides Pacific Command (PACOM) customers the support necessary to develop the best possible information system security posture. We do this through cooperative examination of their systems to identify and help counter vulnerabilities which could be exploited by an adversary.

CNVT is a section of the National Security Agency's (NSA) Central Security Service Pacific Office (NCPAC). Our teams are made up of personnel from the NSA's Network Attack Techniques (C44) and Information Assurance (F405) divisions, which occasionaly supplemented by personnel from the U.S. Navy (including USCINCPAC(J65) and NPS staff).

We encourage you to learn more about CNVT's service.

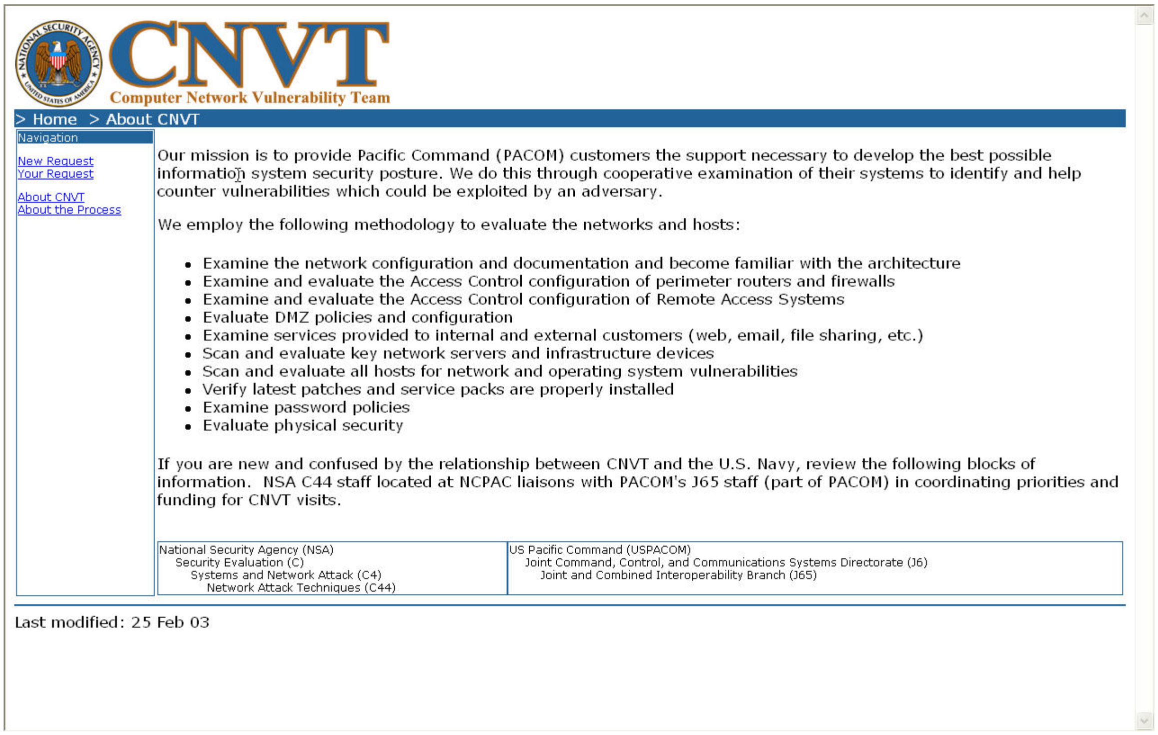
If you're interested in our data collection process, we have an overview for you.

Our address:
NSA/CSS Pacific (NCPAC)
Computer Network Vulnerability Team
PO Box 64028
Camp Smith, HI 96861

(808) 477-3371 (Commercial/STU-III)
(808) 477-3350 (Commercial fax)

Last modified: 25 Feb 03

CNVT Home Page



Our mission is to provide Pacific Command (PACOM) customers the support necessary to develop the best possible information system security posture. We do this through cooperative examination of their systems to identify and help counter vulnerabilities which could be exploited by an adversary.

We employ the following methodology to evaluate the networks and hosts:

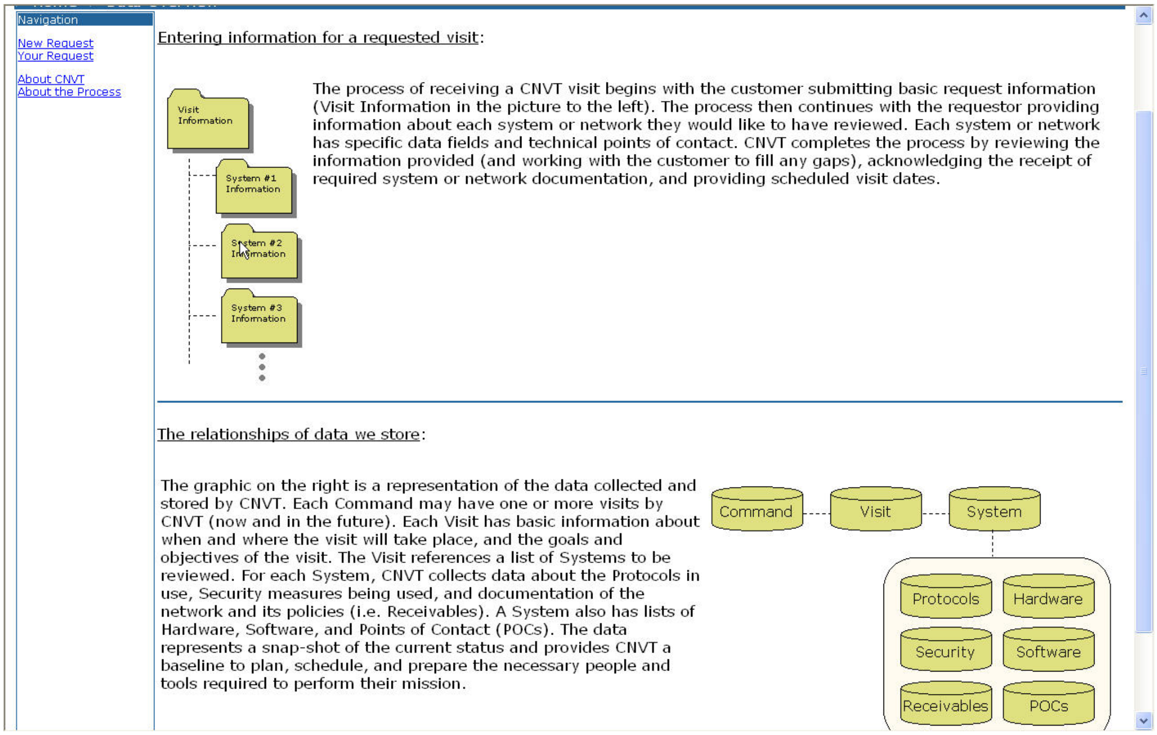
- Examine the network configuration and documentation and become familiar with the architecture
- Examine and evaluate the Access Control configuration of perimeter routers and firewalls
- Examine and evaluate the Access Control configuration of Remote Access Systems
- Evaluate DMZ policies and configuration
- Examine services provided to internal and external customers (web, email, file sharing, etc.)
- Scan and evaluate key network servers and infrastructure devices
- Scan and evaluate all hosts for network and operating system vulnerabilities
- Verify latest patches and service packs are properly installed
- Examine password policies
- Evaluate physical security

If you are new and confused by the relationship between CNVT and the U.S. Navy, review the following blocks of information. NSA C44 staff located at NCPAC liaisons with PACOM's J65 staff (part of PACOM) in coordinating priorities and funding for CNVT visits.

National Security Agency (NSA) Security Evaluation (C) Systems and Network Attack (C4) Network Attack Techniques (C44)	US Pacific Command (USPACOM) Joint Command, Control, and Communications Systems Directorate (J6) Joint and Combined Interoperability Branch (J65)

Last modified: 25 Feb 03

CNVT Mission Page



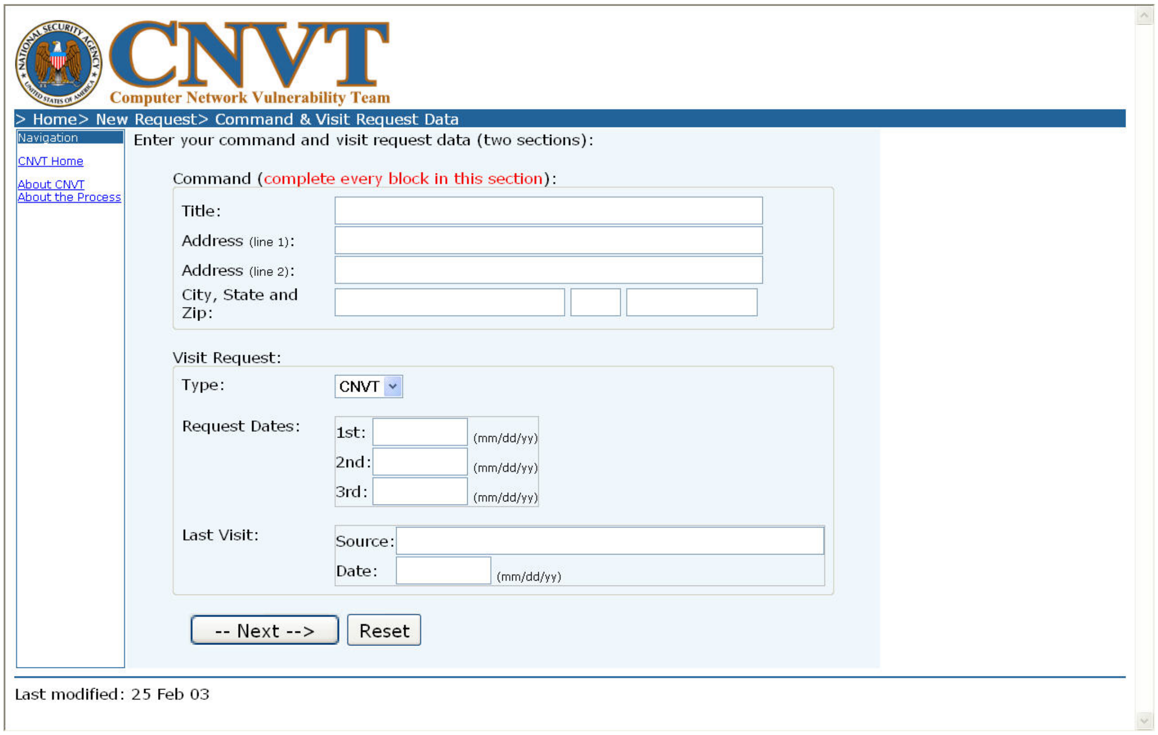
Entering information for a requested visit:

The process of receiving a CNVT visit begins with the customer submitting basic request information (Visit Information in the picture to the left). The process then continues with the requestor providing information about each system or network they would like to have reviewed. Each system or network has specific data fields and technical points of contact. CNVT completes the process by reviewing the information provided (and working with the customer to fill any gaps), acknowledging the receipt of required system or network documentation, and providing scheduled visit dates.

The relationships of data we store:

The graphic on the right is a representation of the data collected and stored by CNVT. Each Command may have one or more visits by CNVT (now and in the future). Each Visit has basic information about when and where the visit will take place, and the goals and objectives of the visit. The Visit references a list of Systems to be reviewed. For each System, CNVT collects data about the Protocols in use, Security measures being used, and documentation of the network and its policies (i.e. Receivables). A System also has lists of Hardware, Software, and Points of Contact (POCs). The data represents a snap-shot of the current status and provides CNVT a baseline to plan, schedule, and prepare the necessary people and tools required to perform their mission.

CNVT Process Page


CNVT
Computer Network Vulnerability Team
> Home> New Request> Command & Visit Request Data
Navigation
CNVT Home
About CNVT
About the Process
-- Next -->
Reset

Enter your command and visit request data (two sections):

Command (complete every block in this section):

Title:

Address (line 1):

Address (line 2):

City, State and Zip:

Visit Request:

Type: CNVT

Request Dates:

1st: (mm/dd/yy)

2nd: (mm/dd/yy)

3rd: (mm/dd/yy)

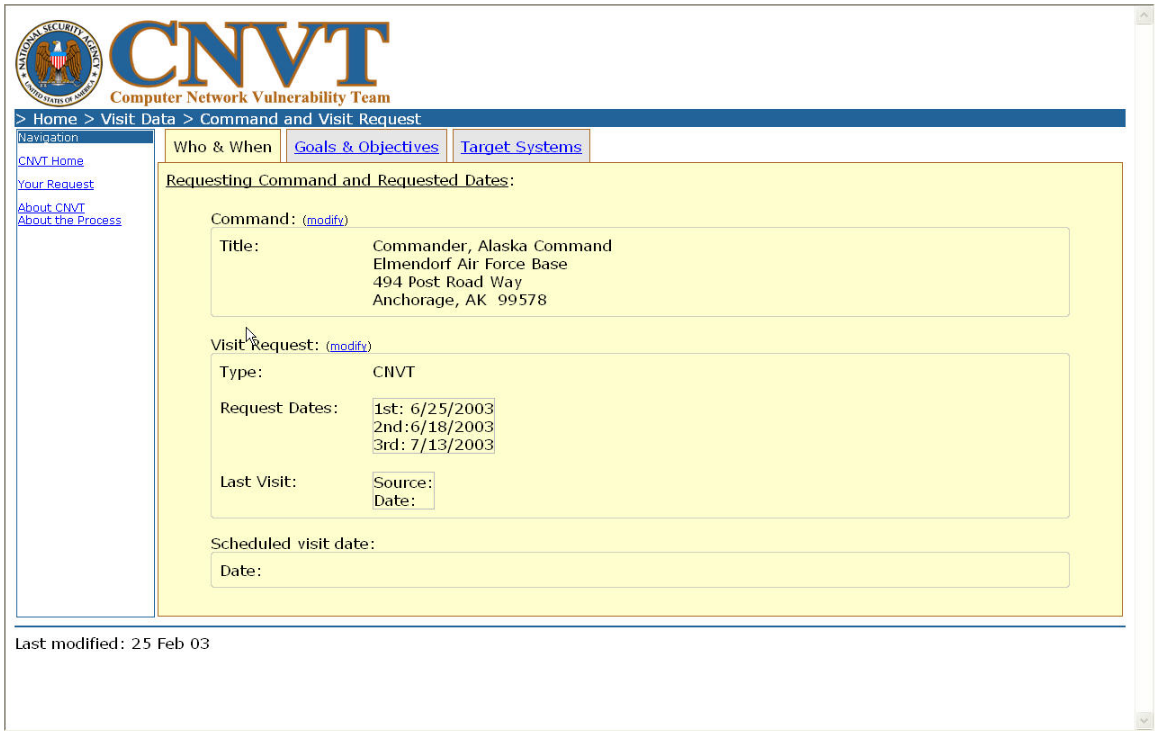
Last Visit:

Source:

Date: (mm/dd/yy)

Last modified: 25 Feb 03

CNVT New Request Page



Requesting Command and Requested Dates:

Command: (modify)

Title: Commander, Alaska Command
Elmendorf Air Force Base
494 Post Road Way
Anchorage, AK 99578

Visit Request: (modify)

Type: CNVT

Request Dates: 1st: 6/25/2003
2nd:6/18/2003
3rd: 7/13/2003

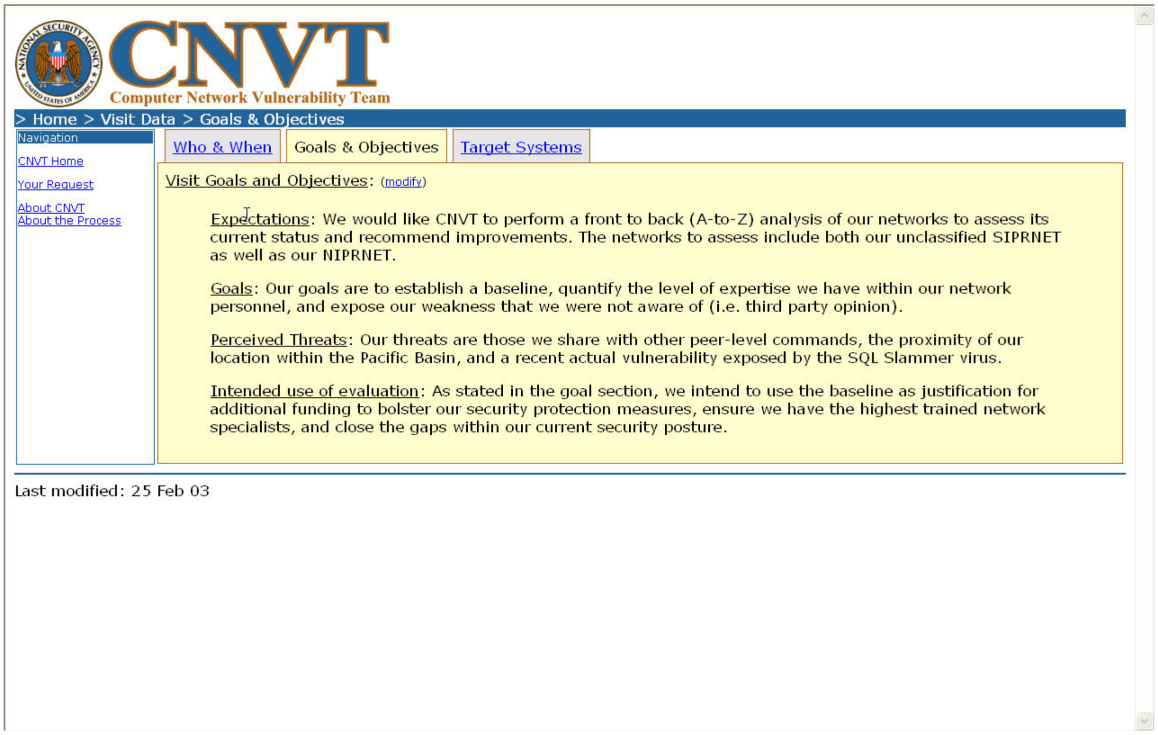
Last Visit: Source:
Date:

Scheduled visit date:

Date:

Last modified: 25 Feb 03

CNVT Info Summary Page



Visit Goals and Objectives: (modify)

Expectations: We would like CNVT to perform a front to back (A-to-Z) analysis of our networks to assess its current status and recommend improvements. The networks to assess include both our unclassified SIPRNET as well as our NIPRNET.

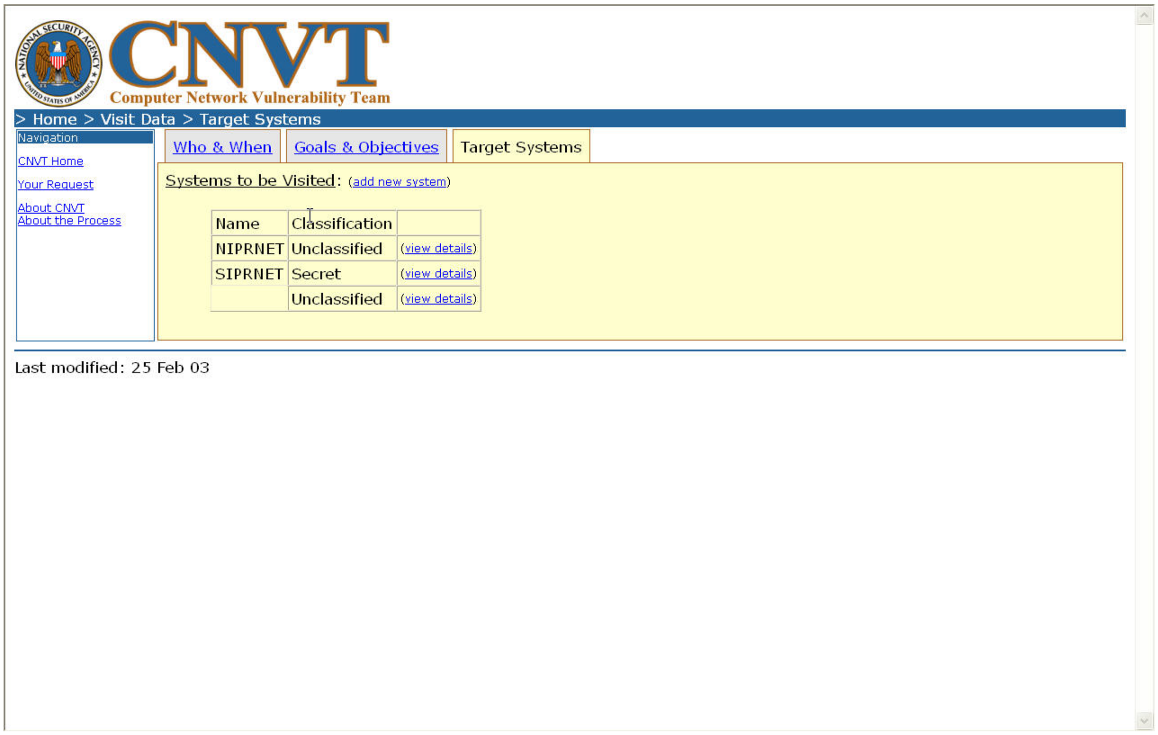
Goals: Our goals are to establish a baseline, quantify the level of expertise we have within our network personnel, and expose our weakness that we were not aware of (i.e. third party opinion).

Perceived Threats: Our threats are those we share with other peer-level commands, the proximity of our location within the Pacific Basin, and a recent actual vulnerability exposed by the SQL Slammer virus.

Intended use of evaluation: As stated in the goal section, we intend to use the baseline as justification for additional funding to bolster our security protection measures, ensure we have the highest trained network specialists, and close the gaps within our current security posture.

Last modified: 25 Feb 03

CNVT Goals and Objectives Page

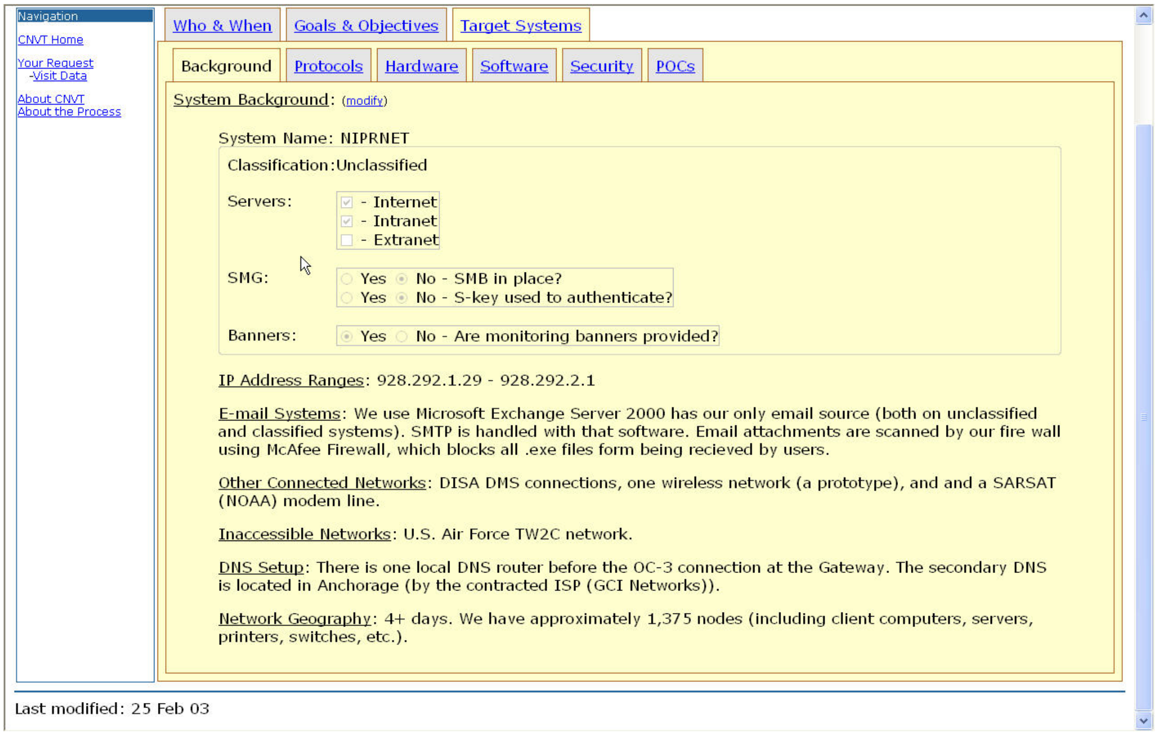


Systems to be Visited: (add new system)

Name	Classification	
NIPRNET	Unclassified	(view details)
SIPRNET	Secret	(view details)
	Unclassified	(view details)

Last modified: 25 Feb 03

CNVT Target Systems Page



System Background: (modify)

System Name: NIPRNET

Classification:Unclassified

Servers: ☑ - Internet
☑ - Intranet
☐ - Extranet

SMG: ○ Yes ● No - SMB in place?
○ Yes ● No - S-key used to authenticate?

Banners: ● Yes ○ No - Are monitoring banners provided?

IP Address Ranges: 928.292.1.29 - 928.292.2.1

E-mail Systems: We use Microsoft Exchange Server 2000 has our only email source (both on unclassified and classified systems). SMTP is handled with that software. Email attachments are scanned by our fire wall using McAfee Firewall, which blocks all .exe files form being recieved by users.

Other Connected Networks: DISA DMS connections, one wireless network (a prototype), and and a SARSAT (NOAA) modem line.

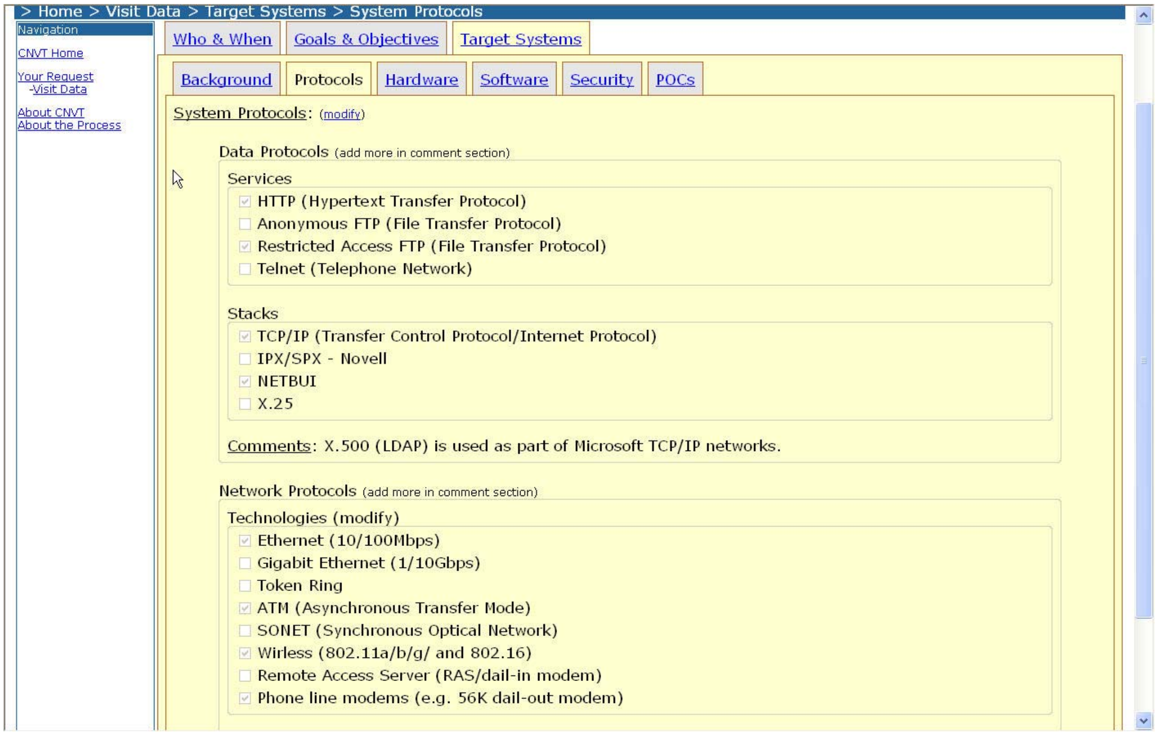
Inaccessible Networks: U.S. Air Force TW2C network.

DNS Setup: There is one local DNS router before the OC-3 connection at the Gateway. The secondary DNS is located in Anchorage (by the contracted ISP (GCI Networks)).

Network Geography: 4+ days. We have approximately 1,375 nodes (including client computers, servers, printers, switches, etc.).

Last modified: 25 Feb 03

CNVT Network Background Page



System Protocols: (modify)

Data Protocols (add more in comment section)

Services

- ☑ HTTP (Hypertext Transfer Protocol)
- ☐ Anonymous FTP (File Transfer Protocol)
- ☑ Restricted Access FTP (File Transfer Protocol)
- ☐ Telnet (Telephone Network)

Stacks

- ☑ TCP/IP (Transfer Control Protocol/Internet Protocol)
- ☐ IPX/SPX - Novell
- ☑ NETBUI
- ☐ X.25

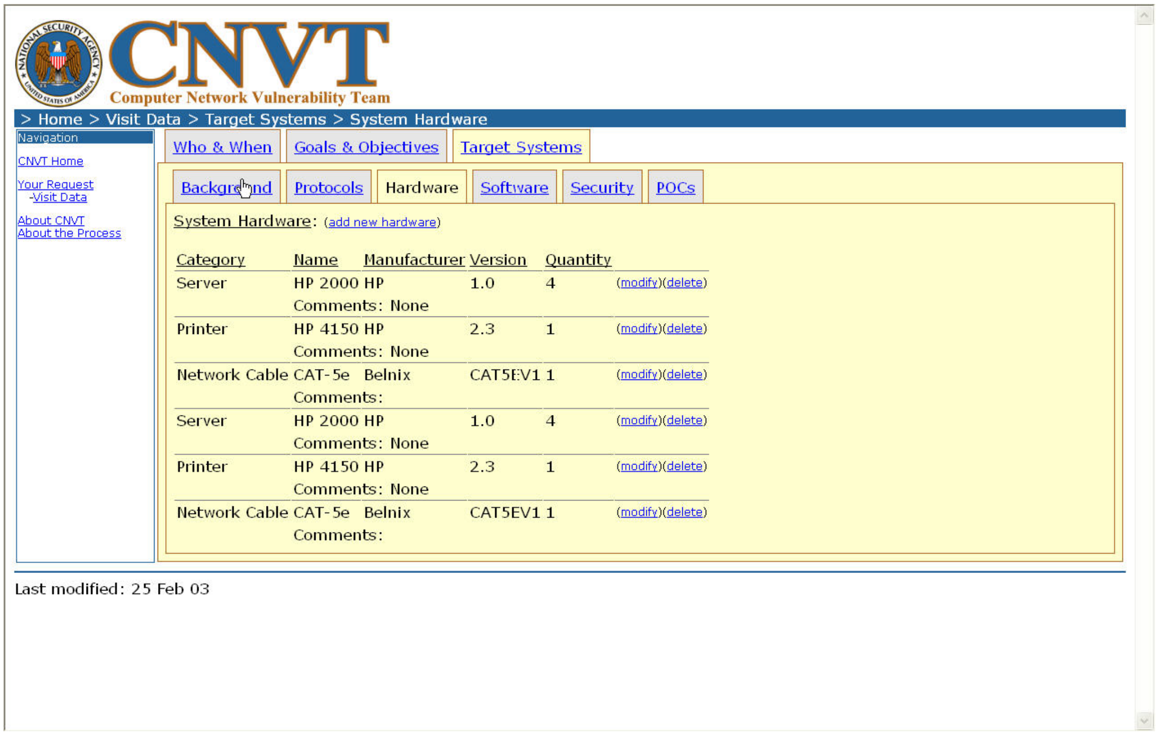
Comments: X.500 (LDAP) is used as part of Microsoft TCP/IP networks.

Network Protocols (add more in comment section)

Technologies (modify)

- ☑ Ethernet (10/100Mbps)
- ☐ Gigabit Ethernet (1/10Gbps)
- ☐ Token Ring
- ☑ ATM (Asynchronous Transfer Mode)
- ☐ SONET (Synchronous Optical Network)
- ☑ Wirless (802.11a/b/g/ and 802.16)
- ☐ Remote Access Server (RAS/dail-in modem)
- ☑ Phone line modems (e.g. 56K dail-out modem)

CNVT Network Protocols Page

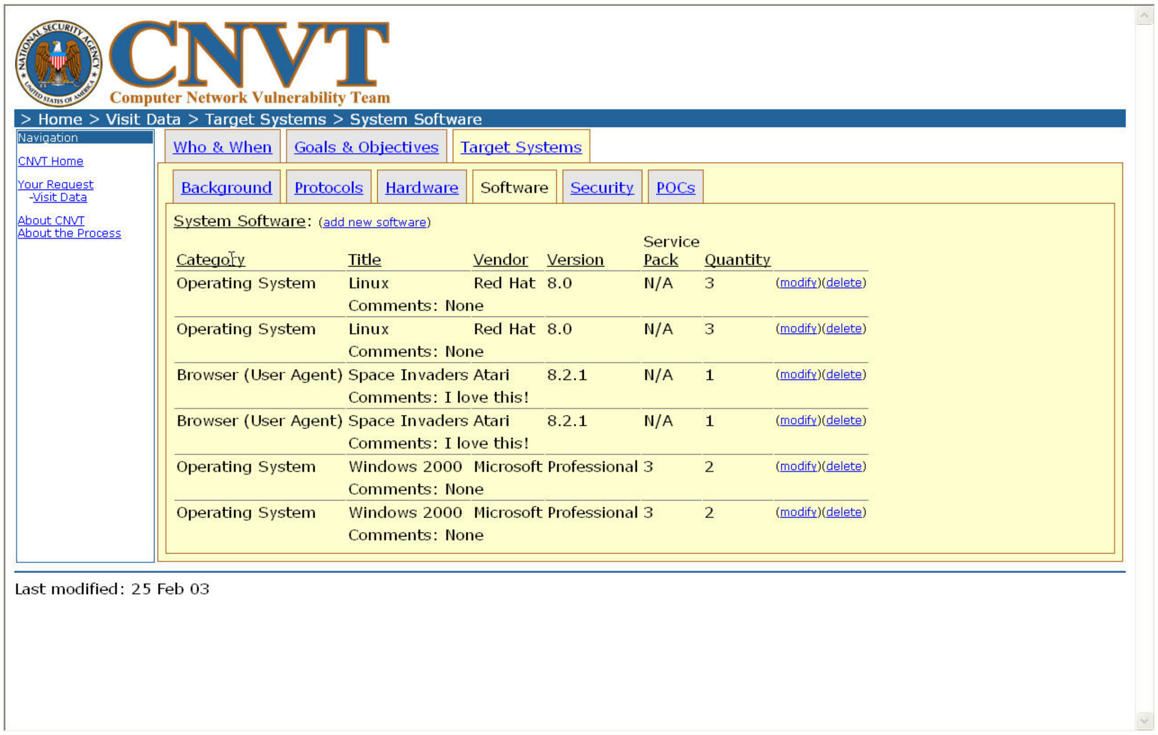


System Hardware: (add new hardware)

Category	Name	Manufacturer	Version	Quantity	
Server	HP 2000	HP	1.0	4	(modify)(delete)
	Comments: None				
Printer	HP 4150	HP	2.3	1	(modify)(delete)
	Comments: None				
Network Cable	CAT-5e	Belnix	CAT5EV1	1	(modify)(delete)
	Comments:				
Server	HP 2000	HP	1.0	4	(modify)(delete)
	Comments: None				
Printer	HP 4150	HP	2.3	1	(modify)(delete)
	Comments: None				
Network Cable	CAT-5e	Belnix	CAT5EV1	1	(modify)(delete)
	Comments:				

Last modified: 25 Feb 03

CNVT Network Hardware Page



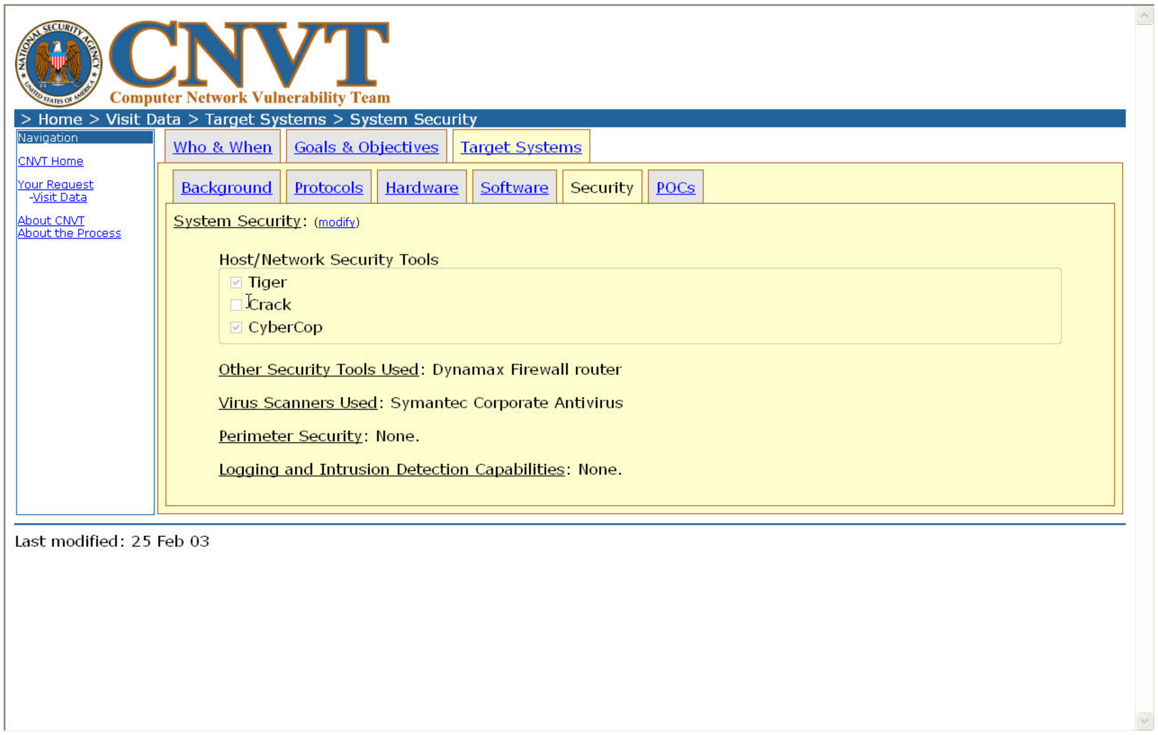
> Home > Visit Data > Target Systems > System Software

System Software: (add new software)

Category	Title	Vendor	Version	Service Pack	Quantity	
Operating System	Linux	Red Hat	8.0	N/A	3	(modify)(delete)
	Comments: None					
Operating System	Linux	Red Hat	8.0	N/A	3	(modify)(delete)
	Comments: None					
Browser (User Agent)	Space Invaders	Atari	8.2.1	N/A	1	(modify)(delete)
	Comments: I love this!					
Browser (User Agent)	Space Invaders	Atari	8.2.1	N/A	1	(modify)(delete)
	Comments: I love this!					
Operating System	Windows 2000	Microsoft	Professional	3	2	(modify)(delete)
	Comments: None					
Operating System	Windows 2000	Microsoft	Professional	3	2	(modify)(delete)
	Comments: None					

Last modified: 25 Feb 03

CNVT Network Software Page



> Home > Visit Data > Target Systems > System Security

System Security: (modify)

Host/Network Security Tools

☑ Tiger
☐ Crack
☑ CyberCop

Other Security Tools Used: Dynamax Firewall router

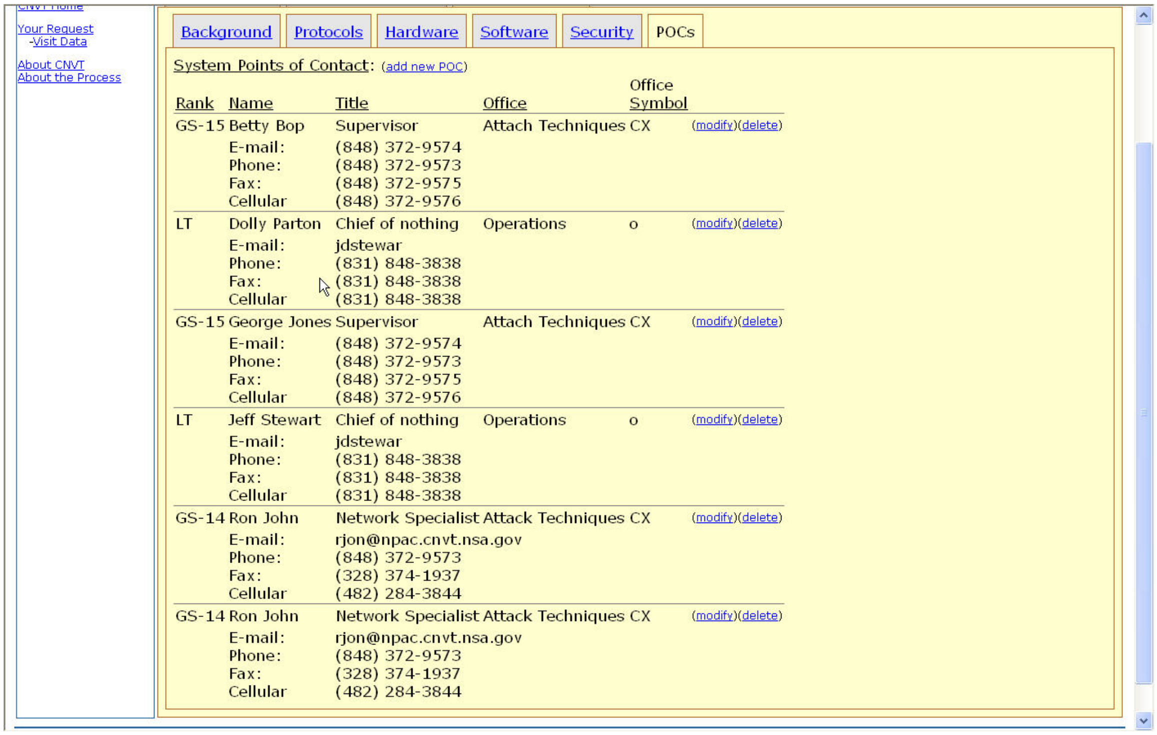
Virus Scanners Used: Symantec Corporate Antivirus

Perimeter Security: None.

Logging and Intrusion Detection Capabilities: None.

Last modified: 25 Feb 03

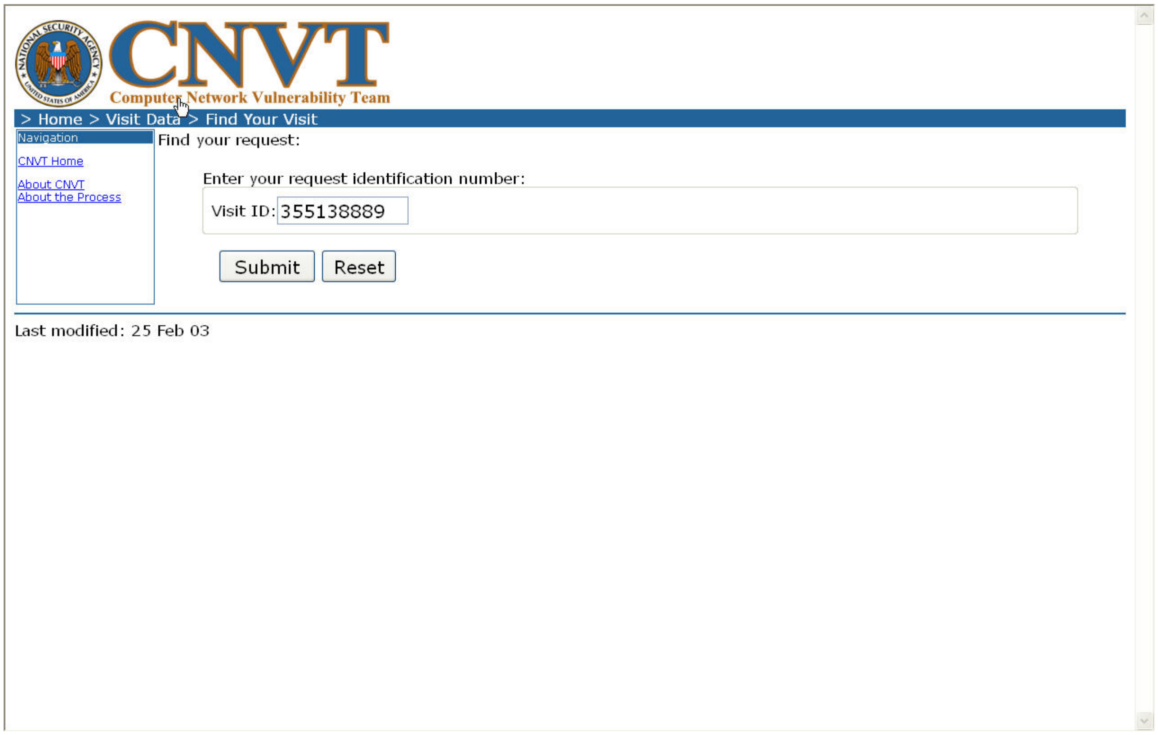
CNVT Network Security Page



System Points of Contact: (add new POC)

Rank	Name	Title	Office	Office Symbol	
GS-15	Betty Bop	Supervisor	Attach Techniques	CX	(modify)(delete)
	E-mail:	(848) 372-9574			
	Phone:	(848) 372-9573			
	Fax:	(848) 372-9575			
	Cellular	(848) 372-9576			
LT	Dolly Parton	Chief of nothing	Operations	o	(modify)(delete)
	E-mail:	jdstewar			
	Phone:	(831) 848-3838			
	Fax:	(831) 848-3838			
	Cellular	(831) 848-3838			
GS-15	George Jones	Supervisor	Attach Techniques	CX	(modify)(delete)
	E-mail:	(848) 372-9574			
	Phone:	(848) 372-9573			
	Fax:	(848) 372-9575			
	Cellular	(848) 372-9576			
LT	Jeff Stewart	Chief of nothing	Operations	o	(modify)(delete)
	E-mail:	jdstewar			
	Phone:	(831) 848-3838			
	Fax:	(831) 848-3838			
	Cellular	(831) 848-3838			
GS-14	Ron John	Network Specialist	Attack Techniques	CX	(modify)(delete)
	E-mail:	rjon@npac.cnvt.nsa.gov			
	Phone:	(848) 372-9573			
	Fax:	(328) 374-1937			
	Cellular	(482) 284-3844			
GS-14	Ron John	Network Specialist	Attack Techniques	CX	(modify)(delete)
	E-mail:	rjon@npac.cnvt.nsa.gov			
	Phone:	(848) 372-9573			
	Fax:	(328) 374-1937			
	Cellular	(482) 284-3844			

CNVT Network POC's Page


CNVT
Computer Network Vulnerability Team
> Home > Visit Data > Find Your Visit
Navigation
CNVT Home
About CNVT
About the Process
Submit
Reset

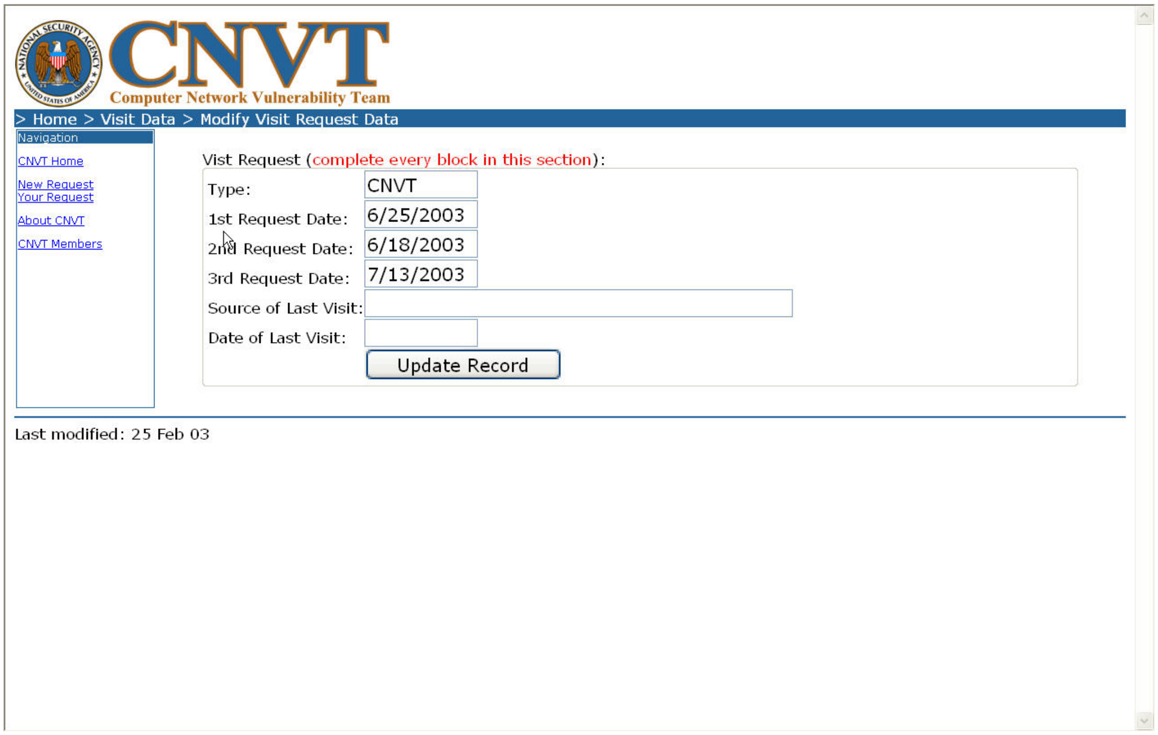
Find your request:

Enter your request identification number:

Visit ID: 355138889

Last modified: 25 Feb 03

CNVT Track a Request Page


CNVT
Computer Network Vulnerability Team
> Home > Visit Data > Modify Visit Request Data
Navigation
CNVT Home
New Request
Your Request
About CNVT
CNVT Members
Update Record

Vist Request (complete every block in this section):

Type: CNVT

1st Request Date: 6/25/2003

2nd Request Date: 6/18/2003

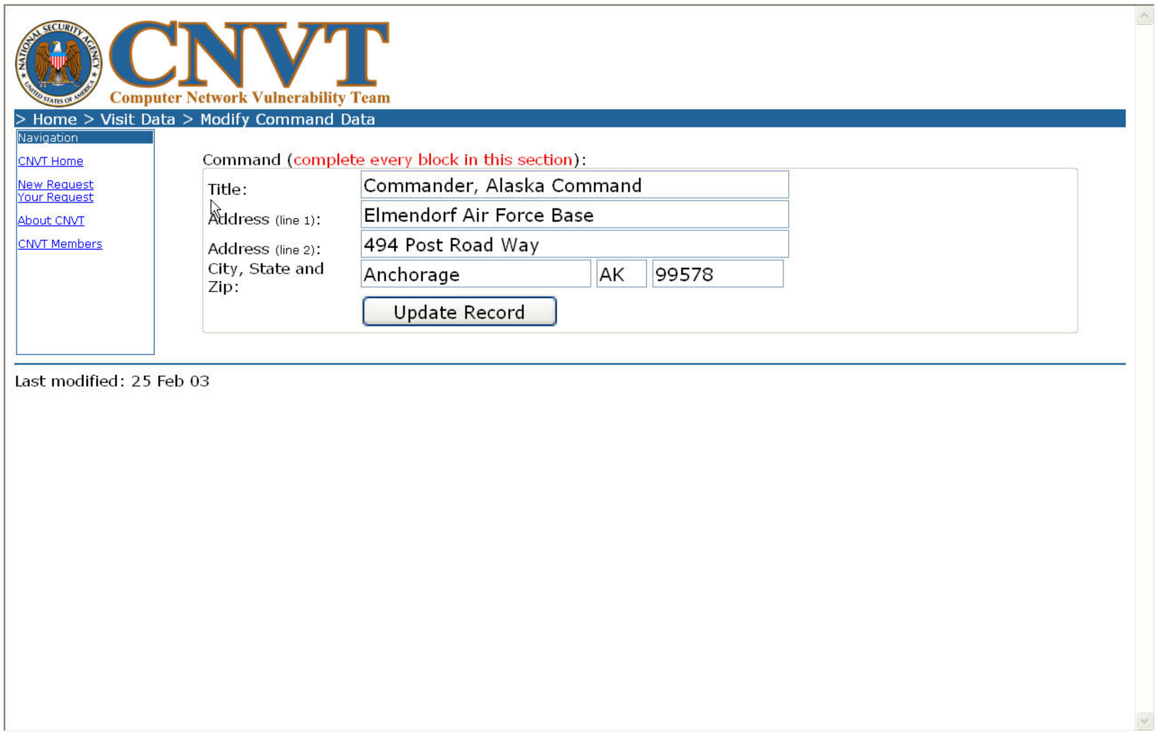
3rd Request Date: 7/13/2003

Source of Last Visit:

Date of Last Visit:

Last modified: 25 Feb 03

CNVT Modify Visit Info Page



Command (complete every block in this section):

Title: Commander, Alaska Command

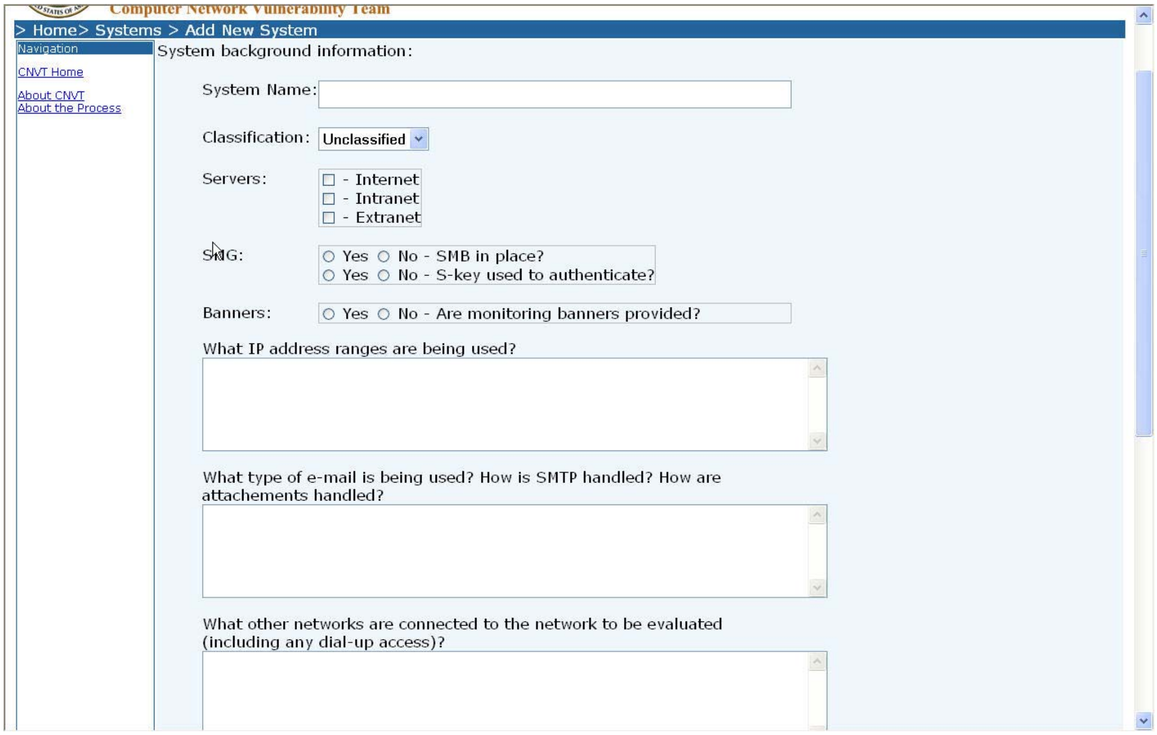
Address (line 1): Elmendorf Air Force Base

Address (line 2): 494 Post Road Way

City, State and Zip: Anchorage AK 99578

Last modified: 25 Feb 03

CNVT Modify Command Info Page



Computer Network Vulnerability Team
> Home> Systems > Add New System
Navigation
CNVT Home
About CNVT
About the Process

System background information:

System Name:

Classification: Unclassified

Servers:
□ - Internet
□ - Intranet
□ - Extranet

SMG:
○ Yes ○ No - SMB in place?
○ Yes ○ No - S-key used to authenticate?

Banners:
○ Yes ○ No - Are monitoring banners provided?

What IP address ranges are being used?

What type of e-mail is being used? How is SMTP handled? How are attachements handled?

What other networks are connected to the network to be evaluated (including any dial-up access)?

CNVT Add New System Page

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Ambrisio, Johanna. "Knowledge Management Mistakes," *Cumputerworld*, July 2000

Benjamins, V. Richard, White Paper, "Knowledge Management in Knowledge Intensive Organizations", December 2001.

Branstetter, Terry L., *Measuring the Value of Graduate Information Technology Education For Marine Officers: A Proof of Concept Study*, Master's Thesis, Naval Postgraduate School, Monterey, California, December 2002.

Conger, Jay A., Gretchen M. Spreitzer, and Edward E. Lawler III. *The Leader's Change Handbook: An Essential Guide to Setting Direction and Taking Action*, Jossey-Bass, 1999.

Davenport, Thomas H. and James E. Short, "The New Industrial Engineering: Information Technology and Business Process Redesign," *Sloan Management Review*, Summer 1990

Davenport, Thomas H. and Michael C. Beers. "Managing Information About Processes," *Journal of Management Information Systems*, Summer 1995.

Davenport, Thomas H., and Lawrence Prusak. *Working Knowledge: How Organizations Manage What They Know*. Cambridge, Massachusetts: Harvard Business School Press 1998

Denning, Dorothy E., *Information Warfare and Security*, The Association for Computing and Addison-Wesley, 1999.

Department of Defense report to Congress, "Network Centric Warfare". 27 July 2001, [http://www.c3i.osd.mil/NCW/], May 2003

DoD Policies, Procedures and Guidelines for review at Defense-wide Information Assurance Program website, [http://www.c3i.osd.mil/org/sio/ia/diap/infocentrall/html#Direct], May 2003

Drake, Keith. "Firms, Knowledge and Competitiveness," *The OECD Observer*, no. 211, April-May 1998.

El Sawy, Omar A., *Redesigning Enterprise Processes for e-Business,* McGraw-Hill Irwin, 2001

Espino, James P., *Knowledge Management innovation of the USCG Counternarcotics Deployment Process*, Master's Thesis, Naval Postgraduate School, Monterey, California, September 2000.
Fingar, Peter, and Ronald Aronica. *The Death of 'e' and the Birth of the Real New Economy*, Meghan-Kiffer Press, 2001.

Hammer, Michael, "Reengineering Work: Don't Automate, Obliterate," *Harvard Business Review*, July-August 1990

Housel, Thomas and Valery A. Kanevsky, "Reengineering Business Processes: A Complexity theory Approach to Value Added," *Infor*, 1995

Housel, Thomas J., and Arthur H. Bell., *Measuring and Managing Knowledge,* McGraw-Hill Irwin, 2001.

Krishna, Jayant. "Sowing Seeds of Learning," *Human Capital*, December 2000.
KVA website, [http://www.businessprocessaudits.com], May 2003

Malhotra, Yogesh. "Business Process redesign: An Overview," *IEEE Engineering Management Review*, vol 26, no. 3, Fall 1998.

Malhotra, Yogesh. "Knowledge Management for e-Business Performance," *Information Strategy: The Executives Journal*, Summer 2000

Manasco, Britton. "Leading Firms Develop Knowledge Strategies", *Knowledge, Inc*., 1996, [http://www.webcom.com/quantera/Apqc.html], May 2003

Manasco, Britton. "Leading Companies Focus on Managing and Measuring Intellectual Capital," *Knowledge, Inc*., [http://www.webcom.com/quantera/IC.html], May 2003

Marakas, George M. *Decision Support Systems in the Twenty-First Century,* Prentice Hall, 1999.

Moore, Andy. "Information Rich, Knowledge Poor," A Special White Paper Supplement to *KMWorld*, February 2002.

Navarro, Randall J., *Using Knowledge Management to Innovate U.S. Coast Guard Command Center Processes,* Master's Thesis, Naval Postgraduate School, Monterey, CA, June 2001.

Nonaka, Ikujiro and Hirotaka Takeuchi, *The Knowledge-Creating Company,* The Oxford University Press, 1995.

Northcut, Stephen, et al., *Inside Network Perimeter Security,* New Riders Publishing, 2003.

Osterland, Andrew. “Grey Matters: CFO's Third Annual Knowledge Capital Scorecard”, *CFO Magazine*, April 1, 2001.
Stewart, Thomas A. “The Case Against Knowledge Management”, *Business 2.0,* Febraury 2002, p. 80

Strassman, Paul A. “Measuring and Managing Knowledge Capital,” *Knowledge Executive Report*, June 1999.

Sun Microsystems Self-Assessment Questionnaire, [http://www.sun.com.au/solutions/security/self_assessment.html], June 2003

Tutorial, “Knowledge Value Added Methodology”, International Engineering Consortium, [http://www.iec.org], May 2003

Ulrich, William M. “Taking Another Shot at BPR”, *Computerworld*, December 2000.
Zack, Michael H. “Managing Codified Knowledge,” *Sloan Management Review*, vol 40, no. 4, Summer 1999.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Marine Corps Representative
   Naval Postgraduate School
   Monterey, California

4. Director, Training and Education, MCCDC, Code C46
   Quantico, Virginia

5. Director, Marine Corps Research Center, MCCDC, Code C40RC
   Quantico, Virginia

6. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
   Camp Pendleton, California

7. Dr. Thomas Housel
   Naval Postgraduate School
   Monterey, California

8. Mr. Brian Steckler
   Naval Postgraduate School
   Monterey, California

9. Robin DeStefano
   NSA/CSS Pacific (NCPAC)
   Camp H. M. Smith, Hawaii

10. Anna Louie
    HQ USPACOM J65
    Camp H. M. Smith, Hawaii

11. James Ehlert
    HQ USPACOM J394
    Camp H. M. Smith, Hawaii

12. Dan C. Boger
    Naval Postgraduate School
    Monterey, California